ASAMBLEA NACIONAL DE LA REPÚBLICA DEL ECUADOR

COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN Y SEGURIDAD INTEGRAL

INFORME PARA SEGUNDO DEBATE DEL "PROYECTO DE LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD"

Integrantes de la Comisión:

Inés Margarita Alarcón Bueno - Presidenta
Andrés Felipe Castillo Maldonado – Vicepresidente

Camila Anahí Cueva Toro
Mario Amado Zambrano Vera
Gema Karolina Dueñas Palma
Francisco Andrés Cevallos Macías
Mariana Yumbay Yallico
Gerardo Eugenio Machado Clavijo
Jhajaira Estefanía Urresta Guzmán
Jahiren Elizabeth Noriega Donoso

Quito, 30 de enero del 2026

Tabla de Contenido

1. OBJETO 3
2. ANTECEDENTES 3
2.1. Información sobre la presentación del proyecto, calificación, notificación y avocación de conocimiento por parte de la Comisión. 3
2.2. Referencia general de las principales observaciones realizadas por asambleístas, instituciones y ciudadanos que participaron en el tratamiento. 5
2.3. Observaciones presentadas previo al Informe para Segundo Debate. 5
2.4. Observaciones remitidas durante el proceso de socialización. 52
2.4.1. Observaciones de asambleístas. 53
2.4.2. Observaciones institucionales y ciudadanas. 70
2.5. Detalle de la socialización realizada por la Comisión Especializada Permanente y Ocasional. 102
3. BASE LEGAL PARA EL TRATAMIENTO DEL PROYECTO DE LEY 104
4. ANÁLISIS Y RAZONAMIENTO 107
5. CONCLUSIONES Y RECOMENDACIONES DEL INFORME 117
6. RESOLUCIÓN Y DETALLE DE LA VOTACION DEL INFORME 118
7. ASAMBLEÍSTA PONENTE 118
8. NOMBRE Y FIRMA DE LOS ASAMBLEÍSTAS QUE SUSCRIBEN EL INFORME 118
9. PROYECTO DE LEY DEBATIDO Y APROBADO. 119
10. CERTIFICACIÓN 148

1. OBJETO

El presente documento tiene por objeto poner en conocimiento del Pleno de la Asamblea Nacional el Informe para Segundo Debate del **"Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad"**, calificado por el Consejo de Administración Legislativa y asignado para el tratamiento de la Comisión Especializada Permanente Soberanía, Integración y Seguridad Integral.

2. ANTECEDENTES

2.1. Información sobre la presentación del proyecto, calificación, notificación y avocación de conocimiento por parte de la Comisión.

- Mediante Memorando Nro. AN-TBJE-2024-013-ME, de fecha 03 de septiembre de 2024, el Ing. Johnny Enrique Terán Barragán, en su calidad de Asambleísta por la provincia de Los Ríos, remitió al Presidente de la Asamblea Nacional del Ecuador, en funciones en esa fecha, la iniciativa legislativa correspondiente, adjuntando para el efecto las firmas de respaldo de las y los asambleístas que la apoyan.

- Mediante Memorando Nro. AN-SG-2024-3884-M de fecha 10 de septiembre de 2024, la Secretaría General de la Asamblea Nacional, solicita se proceda con la elaboración del informe de la Unidad Técnica Legislativa previo a la calificación del Consejo de Administración Legislativa.

- Mediante Memorando Nro. AN-SG-UT-2024-0517-M, de 17 de septiembre de 2024, el Coordinador General de la Unidad Técnica Legislativa Dr. Gerardo Vladimir Aguirre Vallejo, remite al Sr. Mgs. Alejandro Xavier Muñoz Hidalgo, Secretario General de la Asamblea Nacional, el Informe Técnico Jurídico No Vinculante Nro. 0318-INV-UTL-AN-2024, de fecha 17 de septiembre de 2024, elaborado por el equipo de la Unidad Técnica Legislativa.

- Mediante Resolución Nro. CAL-HKK-2023-2025-0520 emitida el 19 de septiembre de 2024, el Consejo de Administración Legislativa calificó el "Proyecto de Ley Orgánica de Ciberseguridad", disponiendo remitir a la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, y autorizar para que, de ser el caso se proceda con la unificación del proyecto.

- Mediante Memorando Nro. AN-CSIS-2024-0481-M, de 14 de octubre de 2024, el Abg. Washington Adrian Villafuerte Lara, Secretario Relator, informa a la Secretaria General, sobre el avocamiento de conocimiento del presente proyecto por parte de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral.

- Mediante Memorando Nro. AN-ABIM-2024-0210-ME, de fecha 08 de octubre de 2024, la Sra. Inés Margarita Alarcón Bueno, Asambleísta, remitió a la Presidenta de la Asamblea Nacional del Ecuador, en funciones en esa fecha, la iniciativa legislativa correspondiente, adjuntando para el efecto las firmas de respaldo de las y los asambleístas que la apoyan.

- Mediante Memorando Nro. AN-ABIM-2024-0210-M, de fecha 08 de octubre de 2024, con trámite 456821, la Secretaría General de la Asamblea Nacional, solicita se proceda con la elaboración del informe de la Unidad Técnica Legislativa previo a la calificación del Consejo de Administración Legislativa.

- Mediante Memorando Nro. AN-SG-UT-2024-0603-M, de 16 de octubre de 2024, el Coordinador General de la Unidad Técnica Legislativa, Dr. Gerardo Vladimir Aguirre Vallejo, remite al Sr. Mgs. Alejandro Xavier Muñoz Hidalgo, Secretario General de la Asamblea Nacional, el Informe Técnico Jurídico No Vinculante Nro.- 0385-INV-UTL-AN-2024, de fecha 16 de octubre de 2024, elaborado por el equipo de la Unidad Técnica Legislativa presentado por la asambleísta Inés Margarita Alarcón Bueno.

- Mediante Resolución Nro. CAL-RVVR-2023-2025-0059 emitida el 23 de octubre de 2024, el Consejo de Administración Legislativa calificó el "Proyecto de Ley Orgánica de Protección Digital", disponiendo remitir a la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, y autorizar para que, de ser el caso se proceda con la unificación del proyecto.

- Mediante Memorando Nro. AN-CSIS-2024-0559-M, de 18 de noviembre de 2024, el Mgs. Marco Danilo Jirón Paredes, en su calidad de Secretario Relator, informa a la Secretaría General sobre el avocamiento de conocimiento del presente proyecto por parte de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, así como su unificación con el Proyecto de Ley Orgánica de Ciberseguridad que se encuentra en trámite en esta Comisión.

- Mediante Resolución Nro. 2025-2029-003, el Pleno de la Asamblea Nacional resuelve en lo pertinente: "*Artículo 1.- Los plazos para la tramitación de los informes para primer y segundo debate de las Comisiones Especializadas Permanentes y Ocasionales que a la fecha de inicio del periodo legislativo 2025-2029 hubiesen vencido, tendrán una prórroga de sesenta (60) días, que se contabilizará a partir de la notificación de la presente resolución".*

- Mediante Memorando Nro. AN-CSIS-2025-0365-M, de 26 de julio de 2025, el Mgtr. Marco Danilo Jirón Paredes, Secretario Relator, remite al Mtr. Niels Anthonez Olsen Peet, Presidente de la Asamblea Nacional, informe para primer debate del proyecto denominado: "Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual".

- Mediante Sesión de Pleno de la Asamblea Nacional Nro. 024-AN-2025-2029, de 05 de agosto de 2025, se recibieron observaciones y se dispuso continuar con el trámite correspondiente para la elaboración del informe para segundo debate.

2.2. Referencia general de las principales observaciones realizadas por asambleístas, instituciones y ciudadanos que participaron en el tratamiento.

Durante el proceso de socialización del Proyecto de Ley, se recibió en comisión general a representantes, delegados y delegadas de instituciones, así como expertos en la materia, cuyas intervenciones se sintetizan a continuación:

2.3. Observaciones presentadas previo al Informe para Segundo Debate.

En la siguiente tabla, se resumen las principales observaciones presentadas en Comisión General por distintos actores, provenientes de instituciones públicas y privadas, academia, expertos independientes y actores relevantes de la industria tecnológica.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
Sesión Ordinaria Nro. 20 Fecha: lunes, 18 de agosto de 2025 Modalidad: Semipresencial Link: https://www.facebook.com/100079593587259/videos/24327495313566099 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Asambleísta Lenin Alejandro Lara Pérez	El asambleísta inició su intervención señalando que el proyecto legislativo responde al imperativo de dotar al Estado de un marco normativo robusto y actualizado. Sostuvo que su finalidad es gestionar con eficacia los riesgos en el ciberespacio para salvaguardar los derechos ciudadanos y la integridad de los sectores público y privado. Entre los aportes presentados, destacó la creación del Comité Interinstitucional Especializado de Ciberseguridad (artículo 20-L), un órgano técnico, interinstitucional y permanente, adscrito al ente rector de defensa nacional, con autonomía técnica y funcional, pero sin personería jurídica ni presupuesto propio. La Presidencia del Comité recaería en el ente rector de transformación digital, con el fin de asegurar coherencia con la arquitectura digital del Estado, estandarización técnica y alineación con las políticas de transformación digital. Precisó que los objetivos del Comité comprenden coordinar la respuesta nacional ante incidentes de

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	ciberseguridad, asesorar en políticas públicas y legislación, impulsar la cooperación internacional, fortalecer capacidades institucionales de prevención, detección y respuesta, y representar al Estado en foros internacionales. Destacó que estos objetivos buscan pasar de una gestión fragmentada y sectorial a una acción coordinada, estratégica y de Estado. En cuanto a su conformación, el Comité incluiría representantes de transformación digital, defensa nacional, seguridad interna, relaciones exteriores, UAFE, inteligencia y protección de datos personales, así como invitados con voz pero sin voto, provenientes de organismos multilaterales, agencias de cooperación, universidades, empresas tecnológicas y sociedad civil, garantizando una visión inclusiva y multiactor. Se justificó la participación de estos actores por sus competencias técnicas, de seguridad nacional, cooperación internacional, investigación y protección de derechos digitales. Respecto a sus funciones, el Comité activará protocolos de emergencia frente a incidentes que afecten infraestructuras críticas, servicios públicos o datos personales; creará centros de respuesta en todas las entidades públicas; elaborará y supervisará planes nacionales de ciberseguridad; coordinará cooperación internacional; realizará simulacros; establecerá estándares mínimos de seguridad; y generará lineamientos para la protección de infraestructuras críticas. Estas funciones se articularán con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática, creando una red de defensa digital distribuida y coordinada conforme a estándares internacionales. La secretaría técnica y operativa del Comité estará a cargo del ente rector de defensa nacional, responsable de ejecutar acuerdos, convocar reuniones y consolidar información sobre incidentes. Se estableció que el Comité se reunirá ordinariamente cada tres meses y extraordinariamente en caso de emergencias, con disposiciones transitorias que fijan la instalación en 15 días y la emisión de normativa secundaria en 90 días. Indicó que el diseño institucional se inspira en experiencias comparadas, como el Decreto Ejecutivo 464 en Ecuador y el Comité Interministerial de Ciberseguridad de Chile, combinando la adscripción a defensa nacional, la presidencia en transformación digital

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	y un rol estratégico conforme a la realidad constitucional del país. En materia de cooperación internacional, precisó que el ente rector de transformación digital liderará estas acciones en coordinación con la Cancillería y los ministerios de Defensa Nacional y Seguridad Interna. Destacó que el CSIRT nacional actuará como punto de contacto técnico 24/7, garantizando respuesta inmediata y participación en redes globales, mientras las entidades competentes elaborarán protocolos de investigación y cooperación internacional para delitos informáticos tipificados en el Convenio de Budapest.
Diego Urbina Fletcher, Delegado de Amazon Web Services	El compareciente, en representación de Amazon Web Services, en primer lugar, destacó la necesidad de incorporar una definición de infraestructura crítica digital. Propuso que esta se entienda como el conjunto de instalaciones físicas, redes, sistemas, plataformas, equipos y demás componentes considerados activos de información, necesarios para garantizar la disponibilidad, confidencialidad, integridad y resiliencia de los servicios esenciales. Aclaró que los terceros proveedores de soluciones tecnológicas como servicios de hosting, almacenamiento o procesamiento no deberían ser considerados operadores de infraestructura crítica, pues no proveen directamente servicios esenciales. Asimismo, sugirió definir “servicios esenciales” como aquellos vinculados al funcionamiento del Estado y de los sectores estratégicos reconocidos en la Constitución, tales como los servicios públicos, la salud, las telecomunicaciones, los financieros y otros de carácter prioritario. En segundo lugar, observó que el proyecto menciona tanto a operadores de infraestructura crítica digital como a prestadores de servicios digitales, imponiéndoles obligaciones comunes. Señaló que esta categoría resulta problemática, pues no todo prestador de servicios digitales constituye infraestructura crítica; un ejemplo son las plataformas de pedidos de comida, transporte o entretenimiento, que no deberían asumir cargas regulatorias propias de sectores esenciales. Por ello, recomendó eliminar dicha referencia y centrar el ámbito normativo exclusivamente en operadores de infraestructura crítica digital. Respecto a los reportes de incidentes y sanciones, consideró adecuado que se contemplen medidas correctivas, pero advirtió que la remisión genérica a la

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	"normativa vigente" genera incertidumbre jurídica. Propuso que se especifique el marco sancionatorio aplicable, a fin de brindar claridad a los obligados. En cuanto a la clasificación de infraestructura crítica digital, observó que el proyecto la sujeta a tres factores: impacto potencial de una disrupción, interdependencia con otros sectores y sensibilidad de los datos procesados. Estimó pertinente mantener los dos primeros criterios, pero cuestionó el tercero, pues el manejo de datos sensibles no siempre implica operar infraestructura crítica. Ejemplificó con aplicaciones de transporte que procesan información personal y financiera, pero que no constituyen infraestructura crítica. Recordó que la Ley Orgánica de Protección de Datos Personales ya regula de manera adecuada la protección de datos, por lo que la ley de ciberseguridad debe enfocarse en la defensa de activos e infraestructuras críticas. Finalmente, en relación con la notificación de incidentes, subrayó que esta debe recaer exclusivamente en los operadores de infraestructura crítica. Explicó que, conforme a los contratos vigentes, los proveedores tecnológicos informan al operador, y es este quien reporta al ente rector. Imponer la obligación directa a los proveedores digitales podría generar duplicidades o conflictos, ya que no siempre disponen de la totalidad de la información necesaria para una notificación completa. En conclusión, recalcó que las observaciones planteadas buscan brindar mayor certeza jurídica y delimitar correctamente los sujetos obligados, evitando imponer cargas desproporcionadas a quienes simplemente ofrecen servicios tecnológicos. Insistió en que la ley debe centrarse en los operadores de infraestructura crítica, tanto públicos como privados, para garantizar una protección efectiva de los servicios esenciales del Estado y de la sociedad.
Ab. Juan Francisco Cabezas Martínez **Experto en Derecho Digital y Protección de Datos Personales**	El compareciente, Juan Cabezas Martínez, abogado y máster en Derecho Digital y Sociedad en Red, inició su exposición señalando su experiencia en protección de datos personales y seguridad de la información, así como su trayectoria en estándares internacionales como ISO 27001 e ISO 31700, y su acreditación como aliado en protección de datos conforme al sistema europeo. Expresó que estas credenciales le motivaban a compartir sus observaciones sobre el proyecto de ley en debate. Destacó varias fortalezas del proyecto, entre ellas: la sostenibilidad fiscal al no crear nuevas entidades, asignando competencias al ministerio rector de

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	transformación digital (arts. 6 y 7); el fortalecimiento institucional al consolidar en rango legal lo previsto en el Decreto Ejecutivo 464 sobre el Comité Nacional de Ciberseguridad (arts. 8 al 12); la asignación de roles claros al ente rector (arts. 14 al 19); la creación de un catálogo de infraestructuras críticas digitales; la inclusión de auditorías de seguridad, sistemas de gestión y respuesta a incidentes, y campañas de concienciación; así como la responsabilidad del sector privado bajo estándares internacionales como ISO y NIST. Destacó además el énfasis en la cooperación internacional, especialmente con el Convenio de Budapest y redes como FIRST y RED. Subrayó la necesidad de precisar la definición y categorización de infraestructura crítica, diferenciando, conforme a estándares europeos, entre entidades de categoría uno (esenciales, como energía, salud, transporte y administración pública) y entidades de categoría dos (importantes, como logística, educación, manufactura o servicios digitales). Esta distinción permitiría priorizar recursos, establecer exigencias proporcionales al riesgo y evitar sobrecargar a actores de menor impacto. Planteó la incorporación de la divulgación coordinada de vulnerabilidades (CVD), mediante una base de datos nacional y una política obligatoria para fabricantes que proveen componentes a instituciones de alto riesgo. Esta medida evitaría rezagos frente a estándares globales y fortalecería la capacidad de respuesta temprana. Asimismo, se refirió a la seguridad en la cadena de suministro, señalando que la norma debería exigir trazabilidad del software, incluyendo el uso de un Software Bill of Materials (SBOM). Esto permitiría identificar vulnerabilidades, gestionar dependencias, garantizar actualizaciones y facilitar respuestas rápidas ante incidentes, optimizando así la resiliencia de los sectores críticos. Advirtió que el régimen sancionador requiere mayor claridad. Señaló que la referencia genérica a la “normativa vigente” puede generar inseguridad jurídica y afectar principios constitucionales como el debido proceso. Sugirió adoptar un modelo similar al de la Ley Orgánica de Protección de Datos Personales, con categorías definidas de infracciones y sanciones. Asi también, observó la necesidad de delimitar las competencias del MINTEL y de la Superintendencia de Protección de Datos Personales (SPDP). Explicó que un

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	incidente de ciberseguridad puede involucrar tanto activos críticos como datos personales, lo que podría derivar en conflictos competenciales si no se establecen con claridad los ámbitos de actuación de cada institución. Recomendó que, junto con las obligaciones de cumplimiento, se prevean mecanismos de certificación voluntaria en estándares internacionales, a fin de incentivar la madurez digital y fortalecer el ecosistema de ciberseguridad.
Sesión Ordinaria Nro. 24 Fecha: miércoles, 3 de septiembre de 2025 Modalidad: Presencial Link: https://www.facebook.com/100079593587259/videos/1060486165904380 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Mgtr. Marco Gallardo Ávila – Gerente Nacional de Ciberseguridad y Control de la Corporación Nacional de Telecomunicaciones (CNT EP)	El compareciente, Mgs. Marco Paul Gallardo Ávila, Gerente Nacional de Ciberseguridad y Control de la CNT, inició su intervención destacando su formación como ingeniero en telecomunicaciones, con maestrías en tecnologías de la información y gestión de proyectos, y estudios doctorales en curso. Señaló que posee diversas certificaciones internacionales, entre ellas una de alto nivel en ciberseguridad que solo dos personas en Ecuador ostentan, y que es miembro del grupo de expertos EU Cybernet de la Unión Europea. Recordó que la ciberseguridad constituye hoy un pilar fundamental para todo país, aunque muchas veces su importancia no se percibe hasta que se materializa un ataque. Expuso que ya existen antecedentes graves en la región, como los ocurridos en Costa Rica y en el ejército peruano, e incluso en Ecuador, donde la CNT sufrió un incidente en 2021 que también involucró posteriormente a entidades bancarias. Estos hechos demostraron que un ataque informático puede generar serios problemas a nivel nacional. Subrayó que, aunque la memoria de esos sucesos tiende a diluirse, su impacto en la ciudadanía por la exfiltración de información y registros personales es significativo. Explicó que desde la CNT se han desarrollado simulaciones de ataques para medir la preparación del país. En algunos casos se evidencian respuestas efectivas, pero persisten falencias en varias instituciones, especialmente por la falta de conocimiento homogéneo en ciberseguridad. Señaló que muchas veces se confunden conceptos, como en el caso de la arquitectura “Zero

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	Trust", que en realidad es un modelo de seguridad, pero que algunas empresas comercializan como plataformas específicas. Esta desinformación, dijo, genera dispersión tecnológica y dificulta consolidar una arquitectura nacional de defensa. Indicó que CNT, como empresa pública y proveedora de servicios a numerosas instituciones estatales, busca aportar con asesoría imparcial para orientar la construcción de infraestructuras seguras y resilientes. No obstante, reconoció que Ecuador es uno de los países más atacados en la región, enfrentando millones de intentos diarios. Aclaró que recibir un ataque no significa necesariamente que este se materialice en un incidente, ya que existen mecanismos de contención; sin embargo, insistió en la importancia de socializar y homologar conceptos de ciberseguridad en todo el sector público. Destacó la ausencia de la figura del oficial de seguridad de la información, quien debería reconocerse como punto focal dentro de las instituciones públicas, tal como ocurre con el delegado de protección de datos en la Ley Orgánica de Protección de Datos Personales. También se refirió a las auditorías de seguridad digital, señalando que es necesario definir con claridad si serán ejecutadas por el ente rector o coordinadas con otras instituciones, y qué nivel de especialización deben tener los auditores. Asimismo, valoró positivamente el principio de neutralidad tecnológica, resaltando que la adopción de arquitecturas multivendor reduce la vulnerabilidad frente a fallas en una sola marca, pues la diversidad de proveedores fortalece la resiliencia. Consideró acertada la inclusión de la coordinación operativa en la política de ciberseguridad, pero observó que CNT no había sido considerada dentro de ese marco, a pesar de ser la empresa estatal que presta servicios a la mayoría de entidades públicas y que, tras el incidente de 2021, ha invertido fuertemente en reforzar su seguridad. Subrayó la importancia de la continuidad de negocio, especialmente en servicios públicos, dado que su interrupción afecta no solo a los usuarios, sino también a la imagen internacional del país. Señaló que, aunque Ecuador se encuentra entre los primeros cinco países de la región con mejor capacidad de ciberseguridad, aún existen oportunidades de mejora, particularmente en la homologación de estándares básicos de seguridad en todas las instituciones públicas.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	Destacó, además, el valor de la cooperación internacional. CNT trabaja con Cancillería, MINTEL y otras entidades en proyectos de apoyo y capacitación, y recientemente se integró a FIRST (Fórum of Incident Response and Security Teames), la red mundial de equipos de respuesta a incidentes, con apoyo del MINTEL, EcuCERT y la Escuela Politécnica Nacional. Este paso permitirá elevar el nivel de madurez de la ciberseguridad en el sector público. Reiteró que ninguna institución está completamente exenta de un ataque y que, por ello, la clave está en la capacidad de contención y respuesta. Puso como ejemplo la necesidad de aislar un equipo infectado para evitar la propagación de un virus en toda la institución. Sin embargo, señaló que aún falta priorización presupuestaria y la creación de una arquitectura base que garantice al menos un nivel estándar de resiliencia en todas las instituciones estatales.
Ing. Mariam López – Coordinadora del EcuCERT de la ARCOTEL	La Coordinadora del EcuCERT, Mariam Soraya López, señaló que resulta indispensable que el país adopte una visión sistémica e integral en esta materia, partiendo de una definición clara del ciberespacio. Recordó que, aunque la Política y la Estrategia Nacional de Ciberseguridad hacen referencia al tema, aún no existe una conceptualización legal que precise los cinco actores principales y sus roles. Destacó la importancia de diferenciar la ciberseguridad, centrada en prevención y gestión de incidentes, de los ciberdelitos, que son tipificados penalmente, y subrayó la necesidad de definir claramente qué constituye un ciberdelito y qué se considera infraestructura crítica digital, incluyendo sectores estratégicos y servicios esenciales. Señaló que esta claridad permitiría un levantamiento preciso del catálogo de infraestructuras críticas y su protección. En cuanto al escalamiento de incidentes, explicó que el EcuCERT actúa como coordinador nacional, pese a la creación de un CSIRT nacional bajo la Ley de Transformación Digital, y coordina con el Comando de Ciberdefensa en casos que afectan infraestructura crítica del Estado. Señaló la falta de definiciones claras de ciberdefensa, ciberinteligencia y ciber diplomacia en la legislación, pese a que estos conceptos son fundamentales para la gestión de incidentes y la cooperación internacional. Destacó que Ecuador forma parte del Convenio de Budapest y cuenta con un punto 24/7 de contacto internacional para incidentes transnacionales,

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	aunque carece de protocolos formales para estas articulaciones. Enfatizó la relevancia de los servicios esenciales, como agua y servicios financieros, y la necesidad de definirlos legalmente para articular acciones preventivas y de respuesta. Señaló la importancia de la colaboración público-privada, compartiendo información para alertas tempranas, y mencionó la creación de redes de confianza con instituciones como ASOBANCA. Sobre los objetivos de la ley, propuso ampliar su cobertura para incluir no solo instituciones públicas y privadas, sino también empresas, organizaciones y personas naturales, dado que los incidentes afectan a todo el país. Recomendó clarificar definiciones clave como CSIRT, incidente de seguridad, ciberataque, resiliencia, riesgo, vulnerabilidad y servicio esencial, que permitirán generar normativa secundaria más efectiva. En materia de coordinación y gestión, destacó la necesidad de que el ente rector defina mecanismos claros de coordinación entre CSIRT nacionales y sectoriales, y que se promueva la creación de centros de respuesta en organizaciones con infraestructura crítica. Señaló la importancia de que la inteligencia nacional evalúe amenazas potenciales utilizando técnicas como OSINT (Inteligencia de Fuentes Abiertas) y ciberinteligencia, para generar alertas tempranas y reducir víctimas de ataques como ransomware. Mencionó logros del EcuCERT, como la gestión de incidentes de vulnerabilidades de telecomunicaciones mediante normativa de ARCOTEL, que redujo los incidentes de 200.000 a 20.000 mensuales. Destacó la importancia de notificar incidentes al Centro Nacional de Respuesta y al CSIRT del Comando Conjunto de las Fuerzas Armadas, asegurando rapidez en la respuesta. Señaló que la ley debe incluir cooperación internacional, con la participación de Relaciones Exteriores y la adopción de estándares internacionales (ISO 27000, NIST), adaptados a cada sector y realidad organizacional. Subrayó la necesidad de incluir auditorías de seguridad de la información, medidas correctivas y la obligación de notificar incidentes para generar alertas tempranas. Finalmente, indicó que los prestadores de servicios de telecomunicaciones deben cumplir con directrices técnicas del ente rector en transformación digital, incluyendo restricciones en áreas de seguridad, cerrando

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	así el ciclo de protección de servicios esenciales y fortaleciendo la ciberseguridad nacional.
Sesión Ordinaria Nro. 25 Fecha: jueves, 4 de septiembre de 2025 Modalidad: Presencial Link: https://www.facebook.com/100079593587259/videos/1092037183133559 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Econ. Roberto Romero – Superintendente de Bancos del Ecuador	El representante del sector financiero procedió a dimensionar la magnitud de la red de servicios financieros en Ecuador. Se detalló que, a nivel nacional, el sistema cuenta con más de 177.000 puntos de atención financiera, cifra que incluye oficinas, cajeros automáticos, corresponsales no bancarios y terminales de punto de venta (POS) distribuidos en todas las regiones del país. El argumento central presentado fue que dicha infraestructura opera bajo la supervisión constante en ciberseguridad por parte de la Superintendencia de Bancos. Se enfatizó que esta fiscalización es una labor inherente y permanente de la institución, estableciendo que ya existe una capa fundamental de control sobre el sistema financiero nacional.
Eco. Yesenia Casco, Intendenta de Riesgos, Superintendencia de Bancos del Ecuador	La principal sugerencia transversal fue la de sustituir el término "seguridad" por "seguridad de la información" en todo el cuerpo normativo. Se argumentó que este cambio proporciona una mayor precisión técnica y alinea la ley con los criterios de estándares internacionales reconocidos, como las normas ISO (específicamente la 27032 y 22301) y los lineamientos del Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST). Señaló la necesidad de ajustar y añadir definiciones cruciales en el artículo 5 de la ley para evitar ambigüedades. Sobre Ciberseguridad: Se propuso ampliar la definición actual, reemplazando la frase "en medios digitales" por "en el ciberespacio". La justificación, basada en la norma ISO 27032, es que el ciberespacio es un concepto más amplio que incluye la interacción entre humanos, software y servicios en internet. Como alternativa, se solicitó que, de no aceptarse el cambio, la ley defina explícitamente el alcance de "medios digitales". Sobre Seguridad Digital e Incidentes Digitales: Se requirió que la ley incorpore definiciones formales para

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	los términos "seguridad digital" e "incidentes digitales", ya que actualmente no están definidos. Para "incidentes digitales", incluso se aportó una propuesta de definición basada en la norma ISO 27035, enfocada en eventos que comprometen los activos o las operaciones de una organización. Asimismo, se sugirió ampliar el texto del literal r, para que los lineamientos de gestión de incidentes incluyan la adopción de una estrategia y un marco de ciberseguridad alineado a las mejores prácticas internacionales, garantizando así la preservación de la integridad, confidencialidad y disponibilidad de los activos de información. La propuesta busca que las instituciones públicas cuenten con la capacidad de identificar, proteger, detectar, responder y recuperarse de forma resiliente y oportuna ante amenazas y eventos de ciberseguridad. En el análisis del artículo 20 de la Ley, relativo a los Principios de Ciberseguridad, se recomienda precisar y armonizar conceptos con lo establecido en la Ley Orgánica de Transformación Digital y Audiovisual, así como en el Acuerdo Ministerial 621 del MINTEL. En particular, se sugiere definir en el artículo 5 los términos infraestructura crítica digital, prestadores de servicios digitales y operadores de infraestructura crítica digital, señalando con claridad si el alcance de estas disposiciones se limita al sector público o si incluye también al sector privado. En el literal a. sustituir la referencia a “datos” por “información”, y en el literal c, planteó igual ajuste para reforzar su amplitud conceptual. Además, se sugirió introducir términos como “activos digitales”, “entorno digital” y “procesos digitales”, tomando como referencia la Ley de Transformación Digital y normas ISO pertinentes. También se propuso ajustar los principios de proporcionalidad y resiliencia: en el primero, reemplazar “seguridad” por “seguridad de la información”; y en el segundo, precisar que las capacidades técnicas deben anticipar, resistir, responder y recuperarse de incidentes o ataques, siguiendo modelos internacionales. Respecto al artículo 20-B, se recomendó definir “incidentes digitales” y establecer sus etapas conforme a estándares internacionales (NIST e ISO 27035), así como aclarar si la gestión será exclusiva del sector público o incluirá al privado.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	En el artículo 20-C sugirieron precisar las responsabilidades de los prestadores de servicios digitales y operadores de infraestructura crítica digital, con base en la Ley de Transformación Digital y el Acuerdo Ministerial 6. En relación con el artículo 20 F, relativo a la coordinación operativa para la implementación de la política de ciberseguridad, se sugiere que en el artículo 5 se defina el término "infraestructura crítica digital" y "continuidad operativa de servicios esenciales", o que se haga referencia a los aspectos contemplados sobre infraestructura crítica digital y servicios esenciales en la política de ciberseguridad establecida por el Acuerdo Ministerial 621 del Ministerio de Telecomunicaciones y Sociedad de la Información. Asimismo, se recomienda que estas entidades incluyan la coordinación con los organismos de control, específicamente la Superintendencia de Bancos, siguiendo los criterios establecidos en la Ley Orgánica de Transformación Digital y el Acuerdo Ministerial 6. Adicionalmente, respecto al literal C, se sugiere modificar el párrafo indicando que la notificación de incidentes debe realizarse conforme a los plazos definidos por el ente rector o el organismo de control dentro del ámbito de sus competencias. La omisión injustificada será sancionada de acuerdo con la normativa vigente, considerando que los incidentes de mayor duración requieren un reporte más inmediato que los de menor duración, con el fin de mantener un registro adecuado de todos los incidentes según su tiempo de ocurrencia. Respecto al artículo 20 I, se recomienda que, en materia de fiscalización y medidas, se establezca que, en caso de aplicarse sanciones, el organismo de control será responsable de realizar la fiscalización correspondiente y, posteriormente, informar al ente rector sobre las acciones ejecutadas. De igual manera, en relación con el literal C del artículo 20, se sugiere incorporar la obligación de creación de un CSIRT nacional y sectorial, conforme a lo indicado en la Ley Orgánica Reformatoria. Para las entidades financieras, se establece que la supervisión en materia de ciberseguridad estará a cargo de los organismos de control, específicamente la Superintendencia de Bancos, actuando en coordinación previa con el Comité correspondiente.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
Eco. Ingrid Villacís, Analista de Innovación, Tecnología y Seguridad de Datos Personales, Superintendencia de Protección de Datos Personales	Ingrid Villacís, en representación del Superintendente de Protección de Datos Personales y como analista de la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales. Respecto al artículo 2, indicó que la competencia de elaborar, mantener y actualizar un catálogo nacional de infraestructura crítica digital ha sido asignada al ente rector, MINTEL. No obstante, considera fundamental definir previamente qué se entiende por infraestructura crítica digital y resaltar su carácter estratégico, ya que su afectación podría impactar la soberanía, la economía y la seguridad ciudadana. Por esta razón, sugirió que la administración de estas infraestructuras corresponda al Ministerio de Defensa, en concordancia con el artículo 158 de la Constitución, más que a MINTEL, y propuso eliminar el artículo 20 H en consecuencia. Señaló también la necesidad de evaluar si MINTEL tiene la competencia para realizar auditorías de seguridad digital, dado que estas podrían superponerse con las funciones de la Contraloría General del Estado, cuya auditoría informática fue recientemente reformada mediante el Acuerdo 036-CG-2025. En relación con la política nacional de ciberseguridad, indicó que ya existe mediante el Acuerdo Ministerial 006-2021 y que, en lugar de formular una nueva, debería actualizarse y mantenerse vigente para alinearse con la Ley Orgánica de Protección de Datos Personales y la normativa actual. Realizó observación sobre los principios de ciberseguridad del artículo 3, destacando que la neutralidad tecnológica, tal como está definida, solo evita privilegios a proveedores y no refleja su importancia en garantizar la protección de datos e infraestructuras, ni conecta con la triada de ciberseguridad: confidencialidad, integridad y disponibilidad. En cuanto al artículo 20, relativo a las responsabilidades del sector privado, consideró que la redacción actual es amplia y ambigua, dado que no contempla todas las particularidades de los distintos sectores privados. Sugirió que la redacción sea más general y no taxativa, y que la terminología utilizada se ajuste a las normas ISO y a la normativa legal vigente para mantener coherencia normativa.
Sesión Ordinaria Nro. 26 Fecha: lunes, 8 de septiembre de 2025	

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
Modalidad: Semipresencial Link: https://www.facebook.com/100079593587259/videos/25391327517135932 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Econ. Juan Carlos Urgiles, Gerente General de la Cooperativa de Crédito Jardín Azuayo	Resaltó la importancia del desarrollo de mecanismos virtuales en el país, destacando que estos permiten realizar eventos y trámites de manera más eficiente y económica, aunque subrayó la necesidad de fortalecer los aspectos de seguridad y ciberseguridad. Enfatizó que la innovación tecnológica comienza y termina con las personas, no solo con el hardware o software. La ciberseguridad debe entenderse como un ecosistema que requiere procedimientos claros, formación adecuada y conocimiento de los riesgos por parte de los ciudadanos. Señaló que la mayoría de los incidentes (aproximadamente el 90%) se producen por fallas en los procesos y la capacitación de las personas, más que por problemas tecnológicos. Además, destacó que la inteligencia artificial facilita la suplantación de identidad, lo que hace imprescindible que la educación en seguridad cibernética sea prioritaria en todos los niveles educativos. Recomendó incorporar la ciberseguridad en el sistema educativo, desde el nivel intermedio hasta la universidad, incluyendo la capacitación de funcionarios y ciudadanos sobre riesgos y buenas prácticas. También planteó que la aplicación de medidas de seguridad debe adaptarse al nivel de riesgo de los activos de información de cada institución, evitando la exclusión tecnológica. Por ejemplo, instituciones financieras que manejan grandes transacciones requieren medidas más estrictas que otras con operaciones menos sensibles. Respecto a la infraestructura tecnológica y normativa, señaló la necesidad de fortalecer la capacidad de las instituciones que manejan información crítica, como el sistema financiero, el Registro Civil y el IESS. Indicó que la normativa debería guiarse por estándares internacionales como la ISO 27001, pero adaptándose a la diversidad del país y al nivel de alfabetización digital de la población. Subrayó que las medidas de seguridad deben ser proporcionales al riesgo, considerando la magnitud de las operaciones y el impacto potencial de un incidente. Entre sus observaciones clave, destacó la importancia de diferenciar entre seguridad y control: la primera

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	relacionada con aspectos educativos, normativos y contextuales, y la segunda con el dominio y vigilancia del espacio cibernético. Resaltó la necesidad de promover sistemas electrónicos y de registro como herramientas confiables y seguras, integradas con la cultura y capacidades de la sociedad. Además, propuso la implementación de un sistema de certificación mínimo y ponderado según el riesgo de los activos operativos de empresas e instituciones públicas y privadas, para generar conciencia sobre la gestión de la información y mejorar la protección frente a ciberataques. En conclusión, enfatizó que la educación, capacitación y fortalecimiento de procesos y normativas son fundamentales para proteger la información y prevenir incidentes de ciberseguridad a nivel nacional. Asimismo, subrayó la necesidad de que las medidas sean proporcionales al riesgo, evitando la exclusión tecnológica y promoviendo un sistema seguro, confiable e integrado, que considere tanto los aspectos técnicos como los educativos y culturales de la sociedad.
Polo Fabián Íñiguez Matute, Experto en temas de ciberseguridad	El Sr. Fabián Iñiguez, docente universitario, creador de la primera carrera de Ingeniería en Ciberseguridad en el país, ex CISO de instituciones financieras y ex Subsecretario de Gobierno Electrónico y Registro Civil en el Ministerio de Telecomunicaciones. Al referirse a la Ley de Transformación Digital, señaló errores de redacción en el artículo 7 literal "O", al mencionarse incorrectamente al "centro de respuestas o incidentes de seguridad informática", en lugar del término correcto "centro de respuestas a incidentes de seguridad informática", reconocido internacionalmente. Propuso suprimir esa frase, considerando que la regulación sobre la materia debe constar en otros artículos. En cuanto al artículo 2, manifestó que el concepto de "infraestructuras críticas digitales" carece de definición en la normativa comparada, y recomendó utilizar la noción de "servicios esenciales", en línea con legislaciones como la NIS2 de la Unión Europea o la ley chilena de ciberseguridad. Respecto al literal r del mismo artículo, sugirió reemplazar "incidentes digitales" por "incidentes informáticos" y ampliar los lineamientos para la gestión de incidentes, incorporando las fases de identificación y protección, además de prevención, detección, respuesta y recuperación. Insistió en que el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática debe asumir un rol central y realizar

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	ejercicios periódicos de ciberseguridad, tal como ocurre en prácticas internacionales. Sobre la Ley de Protección de Datos Personales, propuso modificar el artículo 43 para que las notificaciones no se realicen a la Agencia de Regulación y Control de las Telecomunicaciones, sino directamente al Equipo Nacional de Respuesta a Incidentes de Seguridad Informática, dado que la primera no tiene actualmente competencia en la materia. Resaltó también la necesidad de fortalecer la educación en ciberseguridad desde etapas tempranas, proponiendo que en la Ley de Educación Intercultural se incluya, junto a ciencia, tecnología, ingeniería y matemáticas, la ciberseguridad o los riesgos digitales, con el fin de preparar a niños y jóvenes frente a las amenazas tecnológicas. En cuanto a la notificación de incidentes, apoyó su obligatoriedad, pero sugirió que no se limite únicamente a los datos personales, sino que abarque toda la información cuya disponibilidad, confidencialidad o integridad pueda verse comprometida. Asimismo, planteó que en el artículo 20-H se incluya expresamente la práctica de "monitoreo proactivo" como principio de ciberseguridad, y en el artículo 20 -A se precise el alcance de la neutralidad tecnológica, evitando confundirla con neutralidad comercial. Propuso además que en el artículo 20 "J" se establezca la obligación de que cada entidad designe un responsable de seguridad de la información y de ciberseguridad independiente del área de tecnología, siguiendo el modelo aplicado en el sector financiero y público, para garantizar autonomía en la gestión de riesgos. Posteriormente, recomendó la creación de un Consejo Nacional de Ciberseguridad, de carácter consultivo e interdisciplinario, integrado por representantes del sector público y privado, que asesore al ente rector en el análisis de amenazas y la formulación de políticas. Señaló también la importancia de establecer un fondo específico para financiar las acciones de ciberseguridad, ya que sin recursos económicos adecuados no es posible implementar políticas efectivas. Finalmente, planteó la necesidad de fomentar la ciberseguridad colaborativa, habilitando un marco legal que permita a los hackers éticos reportar vulnerabilidades sin riesgo de sanciones, bajo condiciones reguladas como

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	inscripción en un registro oficial, notificación previa al ente rector y ausencia de ánimo fraudulento. Concluyó señalando que no existe duplicidad de competencias con la Dirección Nacional de Registros Públicos y exhortó a consolidar una legislación integral, coherente y moderna en beneficio de la seguridad digital del país.
Sesión Ordinaria Nro. 28 Fecha: miércoles, 10 de septiembre de 2025 Modalidad: Presencial Link: https://www.facebook.com/100079593587259/videos/1774329863183857 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Dr. Héctor Roberto Gordón, Máster en Seguridad Informática	El Dr. Héctor Roberto Jordán inició su intervención señalando que el análisis de la ley de ciberseguridad se centró en la evaluación de los riesgos, que son un factor crucial para la resiliencia y la gestión de la seguridad de la información. Mencionó que el proyecto está bien estructurado y se alinea con estándares y certificaciones internacionales de buenas prácticas, como las Normas de Información y Ciberseguridad (M.I.S) y la ISO 27001. Destacó que la ley aborda elementos fundamentales como la confidencialidad, integridad y disponibilidad de la información, y promueve la cooperación con equipos de respuesta a incidentes a nivel mundial (CERTs). Sostuvo que el país tiene una capacidad técnica limitada para cumplir con las obligaciones de la ley, señalando la carencia de perfiles especializados en sistemas de respuesta inmediata, alerta temprana (SAT) y auditoría, que son cruciales más allá de los perfiles informáticos básicos. Advirtió sobre los vacíos técnicos y retos legales, como la falta de una clara tipificación de ciertos delitos informáticos en el COIP, lo que podría obstaculizar la aplicación de sanciones. También señaló que la ley carece de una definición precisa de los estándares mínimos comunes y de los criterios para clasificar las infraestructuras críticas del país, como los sistemas SCADA en el sector energético e hídrico o la información en hospitales. Argumentó que esta ambigüedad generaría incertidumbre en los sectores estratégicos. Además, expresó su preocupación por los plazos de implementación, que consideró demasiado ajustados (180 días), lo que presenta un gran reto para la capacitación del personal y la adquisición de tecnologías necesarias. Mencionó que el proyecto no aborda claramente la responsabilidad civil por incidentes, lo que podría generar conflictos con otros entes reguladores como ARCOTEL,

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	la Superintendencia de Bancos y la autoridad de protección de datos. En su opinión, la ley debe contemplar acuerdos de nivel de servicio (SLA) y operativos (OLA) para regular la transferencia de riesgos. También cuestionó la proporcionalidad de las sanciones, argumentando que es imposible cuantificar el valor de la información, por lo que las multas no pueden ser uniformes para todas las entidades, sugiriendo que deben diferenciarse según el tamaño y la capacidad de las organizaciones. Advirtió que un ataque masivo, como un DDoS (ataque de denegación de servicio distribuido), podría paralizar los sistemas críticos del país. Concluyó que el éxito de la ley dependerá de una eficacia operativa, una adecuada coordinación interinstitucional y la capacidad de evitar vacíos legales.
Dra. Lorena Naranjo, Experta en Protección de Datos y Derecho Digital	Inició su intervención destacando que el objetivo general de la ley es fomentar la inversión, el empleo y la adopción de medios digitales. Señaló que, dentro de sus objetivos específicos, se encuentra el de fortalecer el ciberespacio ecuatoriano, pero con un enfoque limitado en la seguridad de la información personal de los ciudadanos. Expresó, que el principal problema radica en el objeto de la ley, ya que el enfoque en la información personal es demasiado estrecho. Argumentó que las organizaciones, tanto públicas como privadas, manejan una variedad de datos que van más allá de lo personal, incluyendo información confidencial, modelos de negocios y propiedad intelectual. Este enfoque restrictivo podría generar inconsistencias con la Ley de Protección de Datos Personales y limitar el alcance de la nueva normativa. También analizó el artículo 2 de la ley, que define la seguridad digital como el eje central, lo cual, en su opinión, podría interpretarse de forma limitada, acotándose únicamente a los datos personales. Similarmente, criticó el concepto de ciberseguridad incluido en el artículo 5, que se restringe a los "servicios digitales". A su juicio, esta definición genera contradicciones con el objetivo de promover la transformación digital, que abarca procesos más amplios que solo los servicios digitales. Una de las principales preocupaciones fue la falta de definiciones claras en la ley, que deja elementos esenciales a la normativa secundaria. Puso como ejemplo el Ministerio de Telecomunicaciones (MINTEL) como ente rector, lo cual podría generar un conflicto de

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	intereses. También señaló la vaguedad en la redacción del artículo 7, que encarga al MINTEL la creación de un catálogo nacional de infraestructura crítica digital "en coordinación con las autoridades competentes", sin especificar quiénes son estas autoridades. Sostuvo que este tipo de vacíos son los que causan conflictos de aplicación en la práctica, como la falta de una clara asignación de responsabilidades ante la notificación de incidentes cibernéticos. Comparó esta situación con la Ley Orgánica de Protección de Datos Personales, que sí establece un procedimiento claro para la notificación de incidentes. Advirtió que, si la nueva ley no define responsabilidades claras, los incidentes que no involucren datos personales podrían quedar sin fiscalización. Además, advirtió sobre posibles choques de competencias y la superposición de regímenes sancionatorios con la Superintendencia de Protección de Datos. Subrayó la relevancia del principio de neutralidad tecnológica, que impide privilegiar un estándar sobre otro, aunque la ley mencione la ISO 27000. Concluyó que la falta de definiciones precisas sobre quiénes y cómo deben participar en los comités nacionales de ciberseguridad, así como la vaguedad en la normativa, son elementos que pueden ser usados para eludir responsabilidades.
Sesión Ordinaria Nro. 29 Fecha: martes, 16 de septiembre de 2025 Modalidad: Semipresencial Nota: El contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Dr. José Vásquez, Delegado de la Superintendencia de Economía Popular y Solidaria	La representante de la Superintendencia de Economía Popular y Solidaria, en nombre de la superintendenta Cristina Murillo, señaló que la propuesta busca proteger la infraestructura digital crítica, los datos personales e institucionales, y garantizar la continuidad de los servicios sociales frente a los crecientes riesgos digitales. Propuso que, en el artículo 20, se considere el riesgo de que las entidades especialmente las del sector privado no notifiquen los incidentes informáticos por temor a sanciones, pérdida reputacional o posibles litigios. En este sentido, sugirió incorporar una cláusula de puerto seguro (safe harbor), que establezca que las notificaciones de buena fe o los reportes de incidentes no sean utilizados como prueba de negligencia en procesos judiciales posteriores, siempre que la entidad demuestre haber actuado con diligencia para remediar la falla.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	Esta medida, explicó, fomentaría una cultura de reporte y colaboración en materia de ciberseguridad, en lugar de un enfoque basado exclusivamente en la sanción. Asimismo, respecto a las obligaciones del sector privado, la representante recomendó fortalecer los mecanismos de cooperación público-privada mediante la creación de una plataforma o instancia formal para el intercambio de información sobre amenazas y vulnerabilidades, similar a un centro de intercambio y análisis de información. Indicó que dicha instancia contribuiría a construir confianza y generar un ecosistema de defensa colectiva más eficaz, basado en la colaboración y no únicamente en la fiscalización. Concluyó reiterando la importancia de contar con espacios que permitan compartir datos actualizados sobre ciberamenazas y cibercrímenes, de modo que las acciones institucionales se ajusten a la realidad digital del país.
Abg. Diego Narváez, Coordinador General de Asesoría Jurídica de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo (SOT)	La representación de la SOT, en primer lugar recomendó precisar rigurosamente conceptos como incidente digital, infraestructura crítica digital, resiliencia y neutralidad tecnológica, a fin de evitar ambigüedades interpretativas. Asimismo, sugirió que definiciones clave como activos de información, vulnerabilidades y riesgos sean incorporadas directamente en la ley, sin delegarlas a normativa secundaria, dada su relevancia en la aplicación práctica. Respecto al artículo 2 del proyecto, propuso aclarar la naturaleza y el carácter vinculante de los lineamientos que se emitirán. En relación con las campañas de concienciación y alfabetización digital, recordó la necesidad de articularlas con lo previsto en el artículo 6 de la Ley Orgánica de Transformación Digital y Audiovisual, que establece la conformación del ecosistema de gobierno digital. En cuanto a los principios rectores del proyecto, enfatizó que el principio de confidencialidad debe entenderse desde la perspectiva de protección de la información, evitando su divulgación intencional o accidental. Además, sugirió revisar la aplicación del principio de disponibilidad ante ataques informáticos, considerando los posibles efectos sobre los usuarios. Sobre el principio de proporcionalidad, la institución consideró necesario definir claramente el concepto de sobreprotección y establecer mecanismos de medición de su impacto. Respecto a las responsabilidades de los prestadores de servicios digitales, recomendó determinar el órgano

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	competente para emitir la regulación técnica correspondiente. En cuanto a la notificación obligatoria de incidentes digitales, si bien se valoró positivamente el plazo de 72 horas previsto, propuso incorporar un sistema de clasificación de incidentes bajo, medio y alto riesgo para garantizar una respuesta proporcional y eficaz según la gravedad del caso. Entre los aportes adicionales, sugirió incluir un articulado sobre el financiamiento de proyectos de ciberseguridad, disponiendo que, cuando las entidades públicas identifiquen proyectos estratégicos sin recursos suficientes, el ente rector en transformación digital los evalúe y el Ministerio de Economía y Finanzas priorice la asignación de fondos conforme a la normativa presupuestaria. Los recursos deberían destinarse a infraestructura tecnológica, talento humano especializado y programas de formación y certificación en ciberseguridad. Asimismo, se propuso establecer un acompañamiento técnico especializado a través del ente rector, que disponga de equipos de expertos en ciberseguridad para brindar apoyo temporal a las instituciones públicas en la formulación, ejecución y evaluación de proyectos. Este acompañamiento reforzaría, sin sustituir, las responsabilidades institucionales, garantizando la alineación con la Política Nacional de Ciberseguridad y con estándares internacionales. Finalmente, se planteó la creación de un catálogo de referencias para proyectos de ciberseguridad, elaborado y actualizado por el ente rector, que contenga requerimientos mínimos de hardware y software, perfiles profesionales, procedimientos, y modelos de proyectos tipo. Dicho catálogo serviría como marco de referencia obligatorio para las instituciones públicas, asegurando coherencia técnica y comparabilidad entre proyectos.
Sesión Ordinaria Nro. 32 Fecha: miércoles, 24 de septiembre de 2025 Modalidad: Presencial Nota: El contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Dr. Marco Rodríguez, Presidente de la ASOBANCA	El compareciente inició su intervención explicando que su exposición abordaría dos aspectos: primero, el manejo de la ciberseguridad, continuidad del negocio y gestión del riesgo operativo en el sistema financiero; y segundo, algunas observaciones técnicas al contenido del proyecto normativo.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	Señaló que la pandemia generó un cambio profundo en los hábitos de los usuarios del sistema financiero, acelerando el uso de canales digitales. En el año 2024 se registraron 1.790 millones de transacciones, de las cuales el 58% se realizaron mediante medios digitales, especialmente a través de dispositivos móviles. Este canal, que en 2019 representaba 24 millones de operaciones, alcanzó en 2024 la cifra de 970 millones, lo que evidencia un crecimiento sustancial. Por esta razón, los esfuerzos del sector bancario en materia de ciberseguridad se han concentrado en proteger y garantizar la continuidad de estos servicios digitales. Indicó que la gestión del riesgo operativo en la banca se estructura bajo el modelo de tres líneas de defensa. La primera línea está conformada por las áreas de negocio, responsables de identificar y administrar los riesgos asociados a las operaciones; la segunda línea corresponde a las unidades especializadas en tecnología y ciberseguridad, encargadas de establecer los controles necesarios; y la tercera línea está integrada por auditoría interna, que verifica la eficacia de los procedimientos implementados. A estas tres líneas se suman la supervisión de la Superintendencia de Bancos y la labor de las auditorías externas, que realizan un control adicional e independiente sobre la gestión institucional. Explicó que los procedimientos de seguridad y gestión del riesgo son elaborados y documentados por las áreas técnicas y aprobados por los comités de riesgos, integrados por la alta gerencia y expertos en diversas materias. Los incidentes registrados se analizan y reportan a la Superintendencia de Bancos, entidad que, además de supervisar, posee facultades sancionatorias y disciplinarias frente al incumplimiento normativo, lo que la distingue de otros organismos de control. Destacó que el sistema financiero ecuatoriano opera bajo estándares internacionales, principalmente las normas ISO 27000 y 27001, que regulan la gestión de la ciberseguridad, la protección de datos y la asignación de responsabilidades independientes. Mencionó también la existencia de comités especializados de seguridad de la información que supervisan la labor de los comités tecnológicos, garantizando así un sistema interno de control basado en principios de equilibrio y transparencia. En cuanto a los mecanismos de protección aplicados, explicó que las instituciones financieras utilizan autenticación biométrica, contraseñas de un solo uso (OTP), software antifraude, firewalls, procesos

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	automáticos de bloqueo ante actividades inusuales y cifrado de datos conforme a los más altos estándares internacionales. Subrayó que, aunque las entidades bancarias implementan medidas robustas de seguridad, los usuarios siguen siendo el eslabón más débil de la cadena, por lo que es fundamental que mantengan actualizados sus dispositivos, utilicen antivirus con licencia y eviten compartir información confidencial a través de canales no oficiales. Resaltó que la ciberseguridad en la banca no debe entenderse como un gasto, sino como una inversión estratégica destinada a preservar la confianza de los clientes y la estabilidad del sistema financiero. En este contexto, formuló algunas observaciones al proyecto de ley, recomendando que la gestión y supervisión de la ciberseguridad en el sistema financiero continúe bajo la responsabilidad de la Superintendencia de Bancos, dado su conocimiento técnico y su experiencia en la materia. Asimismo, propuso que la normativa específica para este sector sea emitida por los organismos de control especializados, en coordinación con la política nacional que establezca la ley. De igual manera, sugirió que la obligación de reporte de incidentes informáticos, prevista en el artículo 20 del proyecto, se canalice a través de la Superintendencia, evitando duplicidad de procesos y burocracia, dado que esta institución ya recibe y consolida dicha información. Finalmente, enfatizó que las entidades de supervisión financiera deben conservar la potestad de aplicar las coordinaciones y regulaciones pertinentes dentro de su ámbito de control.
Dra. Lucía Posso Naranjo, Experta en Ciberseguridad	La compareciente inició su intervención destacando la importancia de fortalecer la alfabetización en seguridad digital, la ciberseguridad, la protección de datos personales y la ciudadanía digital como ejes esenciales dentro del proceso de transformación digital del Ecuador. Recordó que durante su gestión legislativa impulsó iniciativas similares, subrayando que el entorno tecnológico afecta directamente la vida de niñas, niños y adolescentes, quienes acceden tempranamente a Internet, muchas veces sin supervisión, lo que los expone a riesgos como el ciberacoso, el grooming, el sexting, la explotación digital y la desinformación. Señaló que, aunque el acceso a Internet brinda oportunidades educativas y de desarrollo, también genera amenazas serias. Citó datos de la ONU y UNICEF que reflejan la magnitud de la exposición de los menores a

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	entornos digitales inseguros y la urgencia de establecer políticas de protección. En este sentido, insistió en que el sistema educativo y las instituciones públicas y privadas deben estar preparadas para prevenir y responder a estos riesgos. Explicó que su propuesta de reforma a los artículos 32 y 33 de la Ley de Transformación Digital busca incorporar la formación en seguridad digital, ciberseguridad y ética digital en las mallas curriculares desde la educación inicial hasta la superior, para promover una ciudadanía digital responsable. Consideró que no basta con desarrollar infraestructura tecnológica, sino que es necesario preparar a la población para habitar el ciberespacio de forma segura, ética y responsable. Asimismo, resaltó que la alfabetización digital contribuye a reducir la violencia en línea, proteger la salud mental de los jóvenes y cumplir compromisos internacionales, como los establecidos en la Convención sobre los Derechos del Niño y la Observación General N.º 25 del 2021, que exhorta a los Estados a garantizar la seguridad digital en el ámbito educativo. En la parte final de su intervención, propuso varios ajustes técnicos al proyecto de ley, entre ellos la revisión del texto introductorio para mantener coherencia normativa, la diferenciación conceptual entre seguridad digital y ciberseguridad, y la reorganización temática de las disposiciones en capítulos que aborden principios, seguridad digital, ciberseguridad, régimen sancionador y cooperación internacional. Además, sugirió definir parámetros diferenciados de responsabilidad en el régimen sancionador y revisar el modelo chileno sobre infraestructura crítica por considerarlo más adecuado al contexto ecuatoriano. También planteó incorporar exclusiones expresas para las funciones del Estado que deben mantener independencia, como la judicial, la electoral y la legislativa. Finalmente, propuso fortalecer el CSIRT como núcleo central de prevención, detección y respuesta técnica, articulado a una red nacional e internacional de cooperación público-privada.

Sesión Ordinaria Nro. 33
Fecha: jueves, 29 de septiembre de 2025
Modalidad: Semipresencial
Nota: El contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
Abg. Patricia Falconí, Delegada de la Asociación de Empresas de Telecomunicaciones del Ecuador (ASETEL)	La representante de la Asociación de Empresas de Telecomunicaciones inició su intervención destacando la importancia del trabajo conjunto entre el sector público y privado para construir normativas técnicamente aplicables en materia de ciberseguridad. Señaló que todos los actores del ecosistema digital comparten la preocupación por este tema, pero subrayó que su abordaje debe realizarse de forma técnica, neutral y bajo principios internacionales, como la neutralidad tecnológica y de redes. Añadió que la futura ley sobre ciberseguridad debe ser lo suficientemente amplia y flexible para adaptarse a la evolución de la tecnología y de las amenazas cibernéticas. Indicó que el sector de telecomunicaciones realiza constantemente auditorías y mejoras en sus procesos de ciberseguridad, ya que administra infraestructura crítica que brinda servicios a distintos sectores económicos y sociales. Sin embargo, destacó que el 97% de las vulnerabilidades detectadas a nivel nacional provienen del usuario final, según datos de ARCOTEL y del ECUCERT, lo cual evidencia que sin educación y concienciación ciudadana, la ciberseguridad no puede ser efectiva. En este sentido, insistió en que las políticas públicas deben priorizar la formación de los usuarios, puesto que los errores humanos continúan siendo el principal factor de riesgo. En relación con el contenido del proyecto, se refirió al artículo 20-A, sobre los principios de ciberseguridad. Propuso que, en el literal referente a la disponibilidad de servicios y plataformas digitales, se incluya la exigencia de una autorización judicial previa para acceder a la información, a fin de evitar vulneraciones a derechos constitucionales y a las disposiciones emitidas por la Superintendencia de Protección de Datos Personales. En cuanto al literal sobre la neutralidad tecnológica, recalcó que el Estado no debe imponer tecnologías ni proveedores específicos, ya que esto podría restringir la libertad contractual de las empresas y obstaculizar el desarrollo tecnológico y la interoperabilidad de los sistemas existentes. También abordó el artículo 20-I, relativo a la fiscalización y las medidas correctivas, advirtiendo que su redacción actual podría generar rigidez en la aplicación de disposiciones técnicas. Explicó que, debido a la naturaleza cambiante de las tecnologías, las medidas deben ser de carácter orientativo y no obligatorio, evitando que el ente rector imponga soluciones específicas que podrían no ser compatibles con las

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	infraestructuras de los operadores. A modo de ejemplo, señaló que una disposición que obligue a adoptar un software determinado podría ser inviable técnica o financieramente para algunos operadores. Enfatizó que las recomendaciones del ente rector deben ser generales, técnicas, proporcionales y basadas en estándares internacionales, garantizando además un proceso administrativo que respete el principio de contradicción. Concluyó destacando que ningún sistema tecnológico opera de manera aislada, sino que todos forman parte de una red interconectada, por lo que las políticas de ciberseguridad deben promover la interoperabilidad y la cooperación, asegurando medidas técnicamente fundamentadas y sostenibles.
Sr. Andrés Vega, Director de Asuntos Regulatorios de la Cámara de Innovación y Tecnología Ecuatoriana (CITEC)	El representante del sector tecnológico inició su intervención celebrando la decisión de reformar la Ley Orgánica de Transformación Digital y Audiovisual, en lugar de crear una nueva normativa independiente, ya que esto contribuye a reducir la dispersión normativa que afecta al sector. Señaló que, con frecuencia, las empresas tecnológicas deben revisar múltiples marcos legales para cumplir con diferentes exigencias, por lo que esta integración normativa permitirá consolidar un marco más coherente y operativo para el desarrollo digital del país. Planteó cinco observaciones principales. En primer lugar, enfatizó la importancia de contar con definiciones claras sobre los conceptos de “servicios esenciales” e “infraestructura crítica digital”. La falta de precisión, señaló puede generar ambigüedad y extender obligaciones diseñadas para sectores específicos a toda la cadena de servicios digitales, afectando a empresas que no manejan infraestructura crítica. En segundo lugar, abordó la armonización normativa, recordando que el Ecuador ya cuenta con la Ley Orgánica de Protección de Datos Personales y con marcos regulatorios sectoriales emitidos por entidades como la Superintendencia de Bancos y la Superintendencia de Economía Popular y Solidaria. Advirtió que, sin una adecuada articulación entre estas normas, podrían generarse duplicidades o cargas regulatorias innecesarias para los actores tecnológicos. El tercer punto se centró en la ambigüedad de responsabilidades para el sector privado. Explicó que el término “prestadores de servicios digitales” aparece en el texto legal sin una definición clara, lo cual podría implicar obligaciones desproporcionadas para empresas

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	que proveen servicios como almacenamiento en la nube u hospedaje, sin operar infraestructura crítica. Subrayó la necesidad de que las obligaciones recaigan principalmente en los operadores de infraestructura crítica y entidades públicas. También insistió en fortalecer la coordinación interinstitucional con la Superintendencia de Protección de Datos Personales para evitar duplicidades en la presentación de reportes o procedimientos sancionatorios. En cuarto lugar, se refirió a los plazos de adecuación establecidos en las disposiciones transitorias (90 y 180 días), considerándolos insuficientes para que las empresas puedan cumplir con los nuevos requerimientos. Propuso extender dichos plazos a un año, tomando como referencia la Ley Orgánica de Protección de Datos Personales, que otorgó dos años para adecuaciones similares. Señaló que la implementación efectiva de las medidas requiere planificación, inversión y fortalecimiento de capacidades, por lo que imponer tiempos reducidos puede afectar la competitividad del sector. Finalmente, en el quinto punto, advirtió sobre los posibles efectos de una excesiva carga regulatoria en la competitividad e inversión del país. Señaló que la economía digital es global y dinámica, por lo que marcos legales demasiado rígidos podrían desalentar la llegada de inversión extranjera y limitar la innovación tecnológica, en contraposición con las políticas de fomento a la transformación digital impulsadas por el Ejecutivo.
Sesión Ordinaria Nro. 34 Fecha: martes, 7 de octubre de 2025 Modalidad: Semipresencial Link: https://www.facebook.com/100079593587259/videos/790021607229849 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Ing. David Peñafiel, Oficial de Seguridad de la Contraloría General del Estado	El Ing. David Peñafiel, en representación de la Contraloría General del Estado, inició explicando que, si bien la normativa establece que la implementación de estos mecanismos no debe generar un incremento en el gasto público, en la práctica, muchas entidades públicas delegan esta responsabilidad a personal que no pertenece a las áreas de Tecnologías de la Información y Comunicación (TIC). En ese sentido señaló la necesidad de incorporar la figura del “oficial de seguridad de la información”, con

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	formación específica y funciones definidas, pues la actual disposición que permite designar a servidores "no pertenecientes a TIC" resulta contradictoria e insuficiente. Propuso que, para lograr este objetivo sin vulnerar las disposiciones de austeridad, el Ministerio de Trabajo y el Ministerio de Finanzas gestionen los ajustes necesarios para crear y financiar dichas plazas dentro de los estatutos orgánicos institucionales, considerando que la falta de presupuesto constituye una limitación significativa para la adecuada ejecución de estas funciones. Asimismo, respecto al artículo 2 del proyecto indicó que las competencias asignadas al MINTEL deberían incluir la creación y actualización de un catastro nacional de entidades públicas, como base para el catálogo de infraestructura crítica digital. Destacó que este instrumento permitiría avanzar hacia la interoperabilidad y la transformación digital del Estado, al facilitar la conexión y el intercambio seguro de información entre sistemas institucionales. En relación con las auditorías que el MINTEL podría realizar sobre la implementación de la seguridad de la información, advirtió que dicha facultad podría generar conflictos con las competencias de la Contraloría. Explicó que, si bien la CGE se enfoca principalmente en la gestión del gasto público, sería pertinente definir con claridad el alcance de las auditorías del MINTEL, similar a la forma en que el Ministerio de Trabajo ejecuta controles dentro de su ámbito competencial. Recomendó además, que una vez implementado el catastro nacional de entidades públicas, se establezca un sistema de ponderación de incumplimientos normativos para centralizar la información y optimizar los recursos estatales. Propuso que el órgano rector genere estándares técnicos unificados que puedan ser adoptados por todas las instituciones, especialmente aquellas con limitaciones de personal especializado en ciberseguridad. Estos estándares permitirían uniformar procesos, reducir costos y garantizar un nivel mínimo de seguridad. Sobre el ámbito de capacitación, destacó que es fundamental incorporar programas de sensibilización y formación continua para que los funcionarios públicos sepan cómo reaccionar ante incidentes o ataques informáticos. Sin embargo, advirtió que dejar la capacitación al criterio de cada entidad generaría dispersión y desigualdad en la preparación institucional. Por ello, recomendó que el MINTEL diseñe planes y

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	estándares de formación replicables para todas las entidades, y que los resultados de las auditorías puedan servir como insumos para la Contraloría. Respecto a la gestión de incidentes, subrayó que no todas las instituciones públicas cuentan con expertos en ciberseguridad. En consecuencia, planteó la posibilidad de establecer una sectorización estratégica, en la que las entidades con mayor capacidad técnica y tecnológica apoyen a las más pequeñas en tareas de monitoreo y respuesta ante incidentes. Propuso que este esquema sea coordinado por el órgano rector, con un sistema nacional de monitoreo más amplio y robusto, fortaleciendo la labor del ECUCERT. Sobre el artículo 20 C, recomendó precisar las medidas a adoptar para garantizar la seguridad de la información, ya que el texto actual resulta ambiguo. Sugirió que los detalles se definan mediante un reglamento posterior, y que la norma contemple el cumplimiento de estándares internacionales como la ISO 27001, tanto para las entidades estatales como para las que gestionen recursos o servicios públicos. Recordó que existen organismos que ya cuentan con normas específicas como la Superintendencia de Bancos o la Secretaría de Economía Popular y Solidaria, por lo que propuso integrar estos marcos dentro de un Plan Nacional de Transformación Digital y Ciberseguridad, que permita sectorizar las estrategias y fortalecer progresivamente los niveles de protección de todas las instituciones. En relación con la obligación de reporte de incidentes, manifestó que muchas entidades no detectan de inmediato que han sido víctimas de ataques, por lo que una exigencia de reporte en 72h sería inviable. En su lugar, recomendó implementar monitoreos permanentes de infraestructuras críticas, apoyando a las instituciones con menos recursos mediante esquemas de asistencia técnica.
Dra. Sonia Cárdenas, Delegada de la Universidad de las Fuerzas Armadas "ESPE"	La Dra. Sonia Cárdenas, Directora del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas (ESPE). Inició señalando que el proyecto busca establecer un marco normativo moderno y coherente, que fortalezca la protección de los entornos digitales, establezca mecanismos institucionales frente a los riesgos asociados a las Tecnologías de la Información y Comunicación (TIC), y garantice los derechos digitales, la seguridad de la infraestructura crítica y de los servicios esenciales.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	En su revisión, destacó que se descartó la creación de una ley autónoma de ciberseguridad, optando por una reforma a la Ley Orgánica de Transformación Digital y Audiovisual, con el objetivo de evitar duplicidades y superposiciones institucionales y prevenir conflictos de competencia o inconstitucionalidad. Esta decisión permite delimitar la ciberseguridad como un eje técnico, preventivo y estratégico, enfocado en la protección de los activos digitales, la gestión de riesgos tecnológicos y la resiliencia de las infraestructuras críticas. Entre las principales observaciones, señaló que el proyecto no especifica con claridad si la infraestructura crítica a la que se refiere incluye tanto los componentes físicos como digitales, lo que podría generar confusión en su aplicación. Por ejemplo, se hace referencia a la creación de un catálogo nacional de infraestructura crítica digital, sin precisar si se incluyen los sistemas ciberfísicos o de control industrial vinculados a sectores estratégicos como la salud, energía, hidroeléctricas o petróleo. Asimismo, advirtieron que en distintos apartados se alternan los términos activos digitales, activos estratégicos e infraestructura crítica, sin una distinción clara entre elementos digitales y físicos, lo que puede dar lugar a ambigüedades conceptuales y a solapamientos con la seguridad y defensa nacional. En el aspecto conceptual, observó que la definición de ciberseguridad en el texto presenta inconsistencias, al afirmar que “protege la confidencialidad, integridad y disponibilidad de los activos digitales”. Según su criterio, la ciberseguridad garantiza estos principios, mientras que protege los activos que los sustentan, por lo que sugirieron ajustar la redacción para mayor precisión técnica. En relación con el artículo 20 H, relativo a la clasificación de la infraestructura crítica digital, mencionó que el concepto se amplía sin diferenciar adecuadamente entre infraestructura física y digital, pudiendo confundirse con sectores como energía, transporte, agua o salud. En el artículo 20 J, donde se dispone implementar sistemas de gestión de seguridad de la información basados en estándares internacionales como la ISO 27001 o los del NIST, señalaron que se mezclan los conceptos de seguridad de la información y ciberseguridad, los cuales, aunque relacionados, no son equivalentes.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	Precisaron que la seguridad de la información abarca la protección de los datos en todas sus formas (digital y física), mientras que la ciberseguridad se centra exclusivamente en la protección de sistemas y datos en el entorno digital. Por tanto, recomendaron diferenciar ambos enfoques y aclarar a qué norma específica del NIST se hace referencia, dado que esta institución emite múltiples estándares. Respecto del artículo 20 K, que alude a la participación en redes regionales y globales de respuesta a incidentes (CSIRT y CERT), observaron que el texto no establece con claridad los mecanismos de coordinación con el EcuCERT, institución nacional encargada de la respuesta a incidentes de ciberseguridad. Por ello, recomendaron incorporar disposiciones que fortalezcan al EcuCERT, definiendo su rol, funciones y articulación con las demás entidades del sistema. En cuanto al Comité Nacional de Ciberseguridad, señaló que el proyecto no define su composición ni los actores que lo integrarán. Propusieron establecer en la propia ley una composición mínima obligatoria, garantizando la participación del ente rector en transformación digital, los ministerios de Defensa, Gobierno o Interior, Relaciones Exteriores, el Consejo de la Judicatura, la Superintendencia de Bancos, la Superintendencia de Compañías, así como representantes del sector privado y de la academia. Esta estructura multiactor permitiría una gestión integral, técnica y coordinada de la ciberseguridad nacional. Finalmente, recomendaron que la ley consolide un marco de gobernanza integral de la ciberseguridad, con una estructura que evite duplicidades, promueva la cooperación interinstitucional y garantice la protección de los activos digitales y de las infraestructuras críticas.
Sesión Ordinaria Nro. 39 Fecha: jueves, 23 de octubre de 2025 Modalidad: Presencial Link: https://www.facebook.com/100079593587259/videos/1512531486745617 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Antrop. Gabriel Brito, Experto en Seguridad Digital	El investigador Gabriel Brito, antropólogo digital y docente de la Universidad Casa Grande de Guayaquil, inició su intervención presentándose como investigador del Instituto del Internet de la Universidad de Oxford. Explicó que su trabajo se centra en la cultura digital y en

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	la elaboración de políticas públicas orientadas al bienestar digital. En este contexto, expuso su investigación sobre el denominado "Cártel TikTok", un fenómeno transnacional que abarca México, Colombia y Ecuador, y que se ha convertido en un espacio donde organizaciones criminales normalizan la violencia, difunden su agenda y reclutan principalmente a jóvenes y personas vulnerables. Indicó que este fenómeno evidencia los vacíos normativos en materia de ciberseguridad y la falta de mecanismos de protección ciudadana en entornos digitales, los cuales constituyen espacios reales de convivencia y ejercicio de derechos. Destacó que el Estado tiene la obligación de garantizar la seguridad también en estos entornos, mediante medidas integrales que incluyan educación, prevención y alfabetización digital. Advirtió que la moderación de contenido por parte de las plataformas digitales presenta limitaciones, ya que sus políticas centralizadas no se ajustan a los contextos locales. En consecuencia, resulta difícil identificar y controlar contenidos vinculados con el narcoterrorismo o el reclutamiento delictivo. Señaló además que las redes sociales y videojuegos como TikTok, Free Fire o Roblox son actualmente canales utilizados para el reclutamiento criminal de menores, por lo que deben ser considerados dentro del ámbito de la seguridad pública. Explicó que estas prácticas no son nuevas, pues ya fueron empleadas por grupos como ISIS o los cárteles mexicanos, y hoy se reproducen en Ecuador. Citó datos del Observatorio Ecuatoriano de Crimen Organizado, que revelan que el 27% de jóvenes reclutados por bandas delictivas lo fueron mediante redes sociales, y que el 35% de niños y adolescentes utilizan Internet sin supervisión adulta, lo cual aumenta su vulnerabilidad. En este sentido, enfatizó la necesidad de fortalecer la cooperación entre el Estado, otros países y las plataformas tecnológicas para prevenir el reclutamiento digital y proteger a la niñez. Recordó que existen precedentes exitosos, como los acuerdos entre el Ministerio de Asuntos Digitales de Francia y TikTok, que demostraron la posibilidad de regular eficazmente el contenido dañino. Finalmente, recomendó profundizar la alfabetización digital, capacitar a docentes y profesionales en detección de riesgos, promover contenidos positivos que contrarresten las narrativas delictivas y aplicar estrategias

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	de "inoculación informativa" para fortalecer el pensamiento crítico de los jóvenes frente a la desinformación y la manipulación digital. Concluyó que el uso consciente y educativo del Internet puede convertirse en una herramienta de protección y fortalecimiento social.
Sesión Ordinaria Nro. 41 Fecha: 28 de octubre de 2025 Modalidad: Presencial Link: https://www.facebook.com/100079593587259/videos/25066927566249225 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Sr. Mario Cubero, **Experto en Ciberseguridad**	Enfatizó la necesidad de que la reforma incorpore una reestructuración institucional en materia de ciberseguridad dentro del sector público, a través de una gestión interinstitucional efectiva entre el ente rector de ciberseguridad, el Ministerio de Telecomunicaciones y las demás entidades estatales. Sostuvo que, aunque el marco normativo resulta adecuado, la aplicación práctica enfrenta limitaciones, por lo que propuso que las instituciones públicas que administran información sensible como el Registro Civil o la Agencia Nacional de Tránsito cuenten con grupos especializados en ciberseguridad. Citó como ejemplo el caso de la Corporación Nacional de Telecomunicaciones (CNT), que tras sufrir un ataque en 2021 implementó una gerencia técnica de ciberseguridad conformada por un equipo multidisciplinario dedicado a identificar brechas tecnológicas, corregir vulnerabilidades y prevenir incidentes futuros. Asimismo, señaló la necesidad de revisar la figura del oficial de seguridad de la información en las instituciones públicas, ya que este cargo suele ser ocupado por servidores sin perfil tecnológico, lo que dificulta la atención oportuna de los incidentes. En su criterio, las responsabilidades de este funcionario deberían recaer en un equipo especializado que cuente con capacidades técnicas adecuadas para coordinar con el Ministerio de Telecomunicaciones y ARCOTEL. Finalmente, propuso que dicho equipo también asuma la implementación y seguimiento del Esquema de Seguridad de la Información (EGSI) en el sector público, a fin de garantizar una gestión más integral y eficiente de la ciberseguridad estatal.
Sr. Luis Gabriel Cruz Rodríguez, **Experto en Ciberseguridad**	En particular, propuso que en el artículo 20 de la ley se incorpore un nuevo apartado denominado

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	"Ciberseguridad como Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reforma a la Ley Orgánica de Transformación Digital y Audiovisual". Este nuevo artículo explicó tendría como finalidad unificar las disposiciones relacionadas con la protección de sistemas digitales, la prevención de ciberataques y la gestión de riesgos tecnológicos, asegurando así un marco normativo más integral. Asimismo, recomendó que dentro de este artículo se incluya una asignación presupuestaria específica para el fortalecimiento de la ciberseguridad, la protección de datos personales y la seguridad de la información. El especialista destacó que, sin una partida presupuestaria definida, las políticas públicas y los proyectos tecnológicos en materia de ciberseguridad quedan sin ejecución práctica. En ese sentido, propuso que las instituciones públicas incorporen en sus presupuestos institucionales fondos destinados a garantizar la prevención, detección y mitigación de riesgos cibernéticos, así como al fortalecimiento de las capacidades técnicas y humanas. Señaló además que el Ministerio de Economía y Finanzas, junto con el ente rector de la transformación digital, debería establecer los lineamientos técnicos y financieros para la asignación y control de estos recursos, y que el incumplimiento sea considerado una falta administrativa. Mencionó que actualmente el esquema de Seguridad de la Información (EGSI) establece 108 hitos que deben ser cumplidos por las instituciones públicas, pero cuya implementación ha quedado rezagada por falta de recursos. Subrayó que esto limita la capacidad del Estado para desarrollar proyectos tecnológicos efectivos en materia de ciberseguridad y protección de datos. Además, propuso que dentro del apartado de ciberseguridad se amplíen aspectos fundamentales como los principios de ciberseguridad, la gestión de incidentes digitales y las responsabilidades de los prestadores de servicios digitales. Advirtió también la necesidad de revisar la obligación de notificación de incidentes de seguridad contemplada en el artículo 20G del proyecto, debido a posibles conflictos de competencia con la Ley Orgánica de Protección de Datos Personales, que ya regula los plazos y procedimientos de notificación. En ese sentido, explicó que la ley vigente establece un plazo máximo de cinco días para informar sobre vulnerabilidades a las autoridades competentes, mientras que el nuevo proyecto propone un plazo de 72 horas, lo

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	que contradice lo dispuesto en el Código Orgánico Administrativo, que no permite plazos expresados en horas. Finalmente, sugirió fortalecer la composición del Comité Nacional de Ciberseguridad, incorporando al Centro de Inteligencia Estratégica, responsable del análisis y gestión de riesgos en materia de ciberseguridad nacional, y a la Dirección Nacional de Registro de Datos Públicos, además de incluir un delegado especializado en protección de datos personales. Concluyó entregando su documento de observaciones para el respectivo análisis legislativo.
Sr. Omar Durazno, **Experto en Ciberseguridad**	Durante su intervención, presentó cinco observaciones principales respecto al proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, estructuradas en torno a cuatro pilares fundamentales: el ente rector de transformación digital y el Comité Nacional de Ciberseguridad; las políticas, planes y gobernanza; la normativa vigente sobre notificación de incidentes; y la cooperación entre los sectores público, privado e internacional. En primer lugar, destacó la importancia del talento humano como base esencial de la ciberseguridad, señalando que sin personal capacitado no es posible garantizar una protección efectiva frente a amenazas digitales. Mencionó que, a diferencia de países como China, donde se invierte de manera prioritaria en formación especializada, en Ecuador este tema no recibe la atención suficiente. Por ello, propuso actualizar el artículo 7, literal h) o, en su defecto, incorporar un nuevo artículo que disponga la creación de programas de formación en ciberseguridad de alta calidad dirigidos al sector público, privado, operadores de infraestructura crítica y la academia. Estos programas deberían fomentar una cibercultura sostenida a través del sistema educativo y alianzas público-privadas con la participación del Estado, la sociedad civil y la cooperación internacional. Como segunda observación, planteó la necesidad de establecer un modelo de gobernanza en ciberseguridad, ya que actualmente las instituciones responden de manera individual ante los ataques, lo que genera duplicidad de esfuerzos y baja efectividad. Sostuvo que es indispensable articular la gestión entre los sectores público y privado mediante la creación de un marco integral de gobernanza que defina las responsabilidades, coordinación y mecanismos técnicos para la prevención y respuesta ante incidentes. Propuso actualizar el artículo 2,

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	literal u) o incluir un nuevo artículo que formalice esta estructura de gobernanza bajo la rectoría de la autoridad nacional competente. En tercer lugar, recomendó la elaboración de un Plan Nacional de Ciberseguridad, diferenciando este instrumento de la política y la gobernanza. Explicó que la política es la guía estratégica del país, la gobernanza determina quién ejecuta y coordina, y el plan constituye la hoja de ruta operativa. Sugirió incluir un artículo que establezca la creación de este plan como instrumento vinculante, aprobado por el Comité Nacional de Ciberseguridad y ejecutado por la autoridad competente junto con los reguladores sectoriales. La cuarta observación se refirió a la actualización continua de la infraestructura crítica digital. Indicó que los riesgos tecnológicos evolucionan constantemente, por lo que la información y clasificación sobre infraestructura crítica no puede permanecer estática. Propuso actualizar el artículo 20H, incorporando la obligación de revisar de forma semestral y actualizar anualmente dicha clasificación o cada vez que se produzcan cambios significativos, evitando así rezagos que podrían comprometer la seguridad nacional. Finalmente, como quinta observación, propuso fortalecer la asistencia gubernamental ante incidentes cibernéticos. Señaló que, si bien la ley actual exige informar sobre los incidentes, no determina cómo deben gestionarse ni qué entidad brinda apoyo técnico. En ese sentido, sugirió modificar el artículo 20G para permitir que las instituciones puedan solicitar asistencia técnica al ente rector en caso de incidentes graves, sin que esto las exima de sus obligaciones legales. Subrayó que este mecanismo evitaría el “efecto dominó” de contagio entre entidades afectadas y fortalecería la respuesta coordinada del Estado.
Ing. Deysi Espín, Experta en Ciberseguridad	Durante su intervención, enfatizó la importancia del capital humano y de asumir con mayor seriedad la gestión de la seguridad digital, resaltando que cada experto debe tener claridad sobre su nivel de responsabilidad en las distintas etapas del proceso de protección informática. Asimismo, propuso unificar las normativas aplicables al sector público y privado, ya que actualmente existen diferencias significativas entre ambas, lo que dificulta la auditoría y la implementación de medidas homogéneas de seguridad. Señaló que contar con una normativa fija y estandarizada permitiría mejorar la fiscalización y

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	asegurar mayor coherencia en los procedimientos de ciberseguridad. En cuanto al artículo 1 del proyecto, sugirió incorporar de forma expresa los principios de confidencialidad, integridad, disponibilidad y autenticidad de la información, así como la no repudiación de la desinformación procesada, almacenada o transmitida a través de medios digitales y los sistemas que la soportan. Además, propuso añadir las definiciones de "incidente de seguridad digital" e "infraestructura crítica digital" para dotar de mayor precisión técnica al texto legal. Finalmente, respecto al artículo 20-J, recomendó incluir la implementación de sistemas de gestión de seguridad informática basados en estándares internacionales reconocidos, los cuales deberían ser adaptados por el ente rector conforme al nivel de riesgo o criticidad de cada sector. Propuso que se empleen frameworks de referencia, como los basados en normas internacionales de ciberseguridad, o equivalentes, que permitan uniformar las prácticas de protección de la información en las distintas instituciones del país.
Sesión Ordinaria Nro. 42 Fecha: miércoles, 29 de octubre de 2025 Modalidad: Semipresencial Link: https://www.facebook.com/100079593587259/videos/1746293502754094 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Sr. Mario Mayorga, Experto en Ciberseguridad	El Sr. Mayorga realizó observaciones puntuales respecto al tema de los reportes de incidentes, señalando que deberían estructurarse en tres etapas, conforme al alineamiento que actualmente se trabaja en la Unión Europea. Explicó que este modelo contempla una alerta temprana en 24 horas, una notificación en 72 horas y un informe final en un plazo menor a 30 días, el cual debe incluir la causa raíz y las medidas adoptadas. Indicó que este enfoque mejora la trazabilidad y la cooperación operativa. Añadió que, si bien en el texto se contempla el plazo de 72 horas, sería necesario incorporar las otras dos fases para completar el procedimiento técnico. Asimismo, mencionó la importancia de definir un perfil de requisitos de criticidad con tres niveles: básico, medio y alto, que establezcan controles mínimos obligatorios en materia de gestión de riesgos, hardware y cifrado en reposo.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
Sr. Olmedo Narváez, **Experto en Ciberseguridad**	Señaló en relación con el artículo 20-B, referido a la gestión de incidentes digitales, la importancia de incorporar sistemas de alerta temprana que permitan detectar posibles riesgos antes de que ocurran los incidentes. Con base en su experiencia en el ECU-911, enfatizó además la necesidad de establecer, como política obligatoria, la realización de simulacros anuales, con registros auditables que evidencien su cumplimiento y eficacia. En cuanto al artículo 20-C, relativo a las responsabilidades de los prestadores de servicios digitales, propuso que se incluya la obligatoriedad de mantener planes de continuidad operativa y recuperación ante desastres, a fin de garantizar la resiliencia de las plataformas de ciberseguridad. Finalmente, en lo referente a la coordinación estratégica de ciberseguridad, señaló que, si bien se contempla la creación de un Comité Permanente de Ciberseguridad, esta instancia debería actuar en alineación con las directrices del Comité Técnico Permanente de Ciberseguridad, para fortalecer la articulación institucional.
Sr. Kevin Jarre, **Experto en Ciberseguridad**	El compareciente manifestó una observación respecto al artículo 20-J, indicó que esta disposición debería ser más clara y específica en cuanto a los riesgos aplicables a las empresas privadas, considerando que no todas poseen el mismo tamaño ni pertenecen al mismo sector económico. Por ello, sugirió que la normativa sea más explícita y puntual al definir los tipos de riesgos a los que hace referencia.
Sesión Ordinaria Nro. 43 Fecha: miércoles, 29 de octubre de 2025 Modalidad: Semipresencial Link: https://www.facebook.com/100079593587259/videos/861748216243094 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Sr. Ramon Jofree Moreira Pico, **Experto en Ciberseguridad**	El compareciente explicó que su planteamiento busca incorporar cinco artículos enfocados en la educación digital, la formación docente y la coordinación interinstitucional, con el fin de fortalecer la alfabetización digital y reducir los riesgos derivados del factor humano. El primer artículo propone incorporar la educación y ciudadanía digital segura en los niveles de educación básica y bachillerato, con la participación coordinada de

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	los ministerios de Educación, Transformación Digital y Protección de Datos, en concordancia con la Ley Orgánica de Protección de Datos Personales. El segundo plantea la integración curricular de contenidos sobre seguridad digital, tales como protección de datos, contraseñas, ciberacoso, fraudes, higiene digital y uso responsable de la inteligencia artificial. El tercero aborda la formación y actualización profesional docente, priorizando las escuelas públicas y rurales mediante la creación de guías y materiales pedagógicos. El cuarto artículo se refiere a la creación de entornos educativos seguros, con políticas de convivencia digital, medidas técnicas de protección de datos y notificación de incidentes, en concordancia con el artículo 20-G del proyecto. Finalmente, el quinto artículo propone una coordinación interinstitucional y evaluación periódica, con participación del Comité Nacional de Ciberseguridad y elaboración de informes anuales que incluyan indicadores, brechas y avances. Sustentó su propuesta en experiencias internacionales, citando los casos de Reino Unido, Australia, Singapur, la Unión Europea, España, Estonia y Japón, donde la educación en ciberseguridad se imparte desde edades tempranas. Destacó el modelo estonio de "ciberhigiene infantil", que asocia la formación digital al aprendizaje de hábitos básicos como cepillarse los dientes, enfatizando que la prevención temprana fortalece la resiliencia digital nacional. En tal sentido, argumentó que educar desde la niñez puede reducir la superficie de ataque, los costos económicos y el impacto de las vulnerabilidades.
Sr. Alejandro Mero, Experto en Ciberseguridad	El Sr. Mero, estima que el proyecto de ley debería tratarse como una ley independiente y más integral. El enfoque debería centrarse en la prevención y en una respuesta oportuna ante incidentes. En ese sentido, destacó favorablemente la creación de un catálogo nacional y del Comité Nacional de Ciberseguridad. Sin embargo, menciona necesario definir con mayor claridad los roles de las instituciones involucradas. Mencionó que el EcuCERT, entidad dependiente del MINTEL, cumple actualmente funciones de notificación en materia de ciberseguridad; sin embargo, consideró que esta ley debería fortalecer su papel como ente coordinador de los CSIRT nacionales y regionales. Asimismo, sugirió incorporar disposiciones que regulen la cooperación con proveedores internacionales que almacenan datos de las instituciones públicas.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	Finalmente, recomendó que la norma establezca una coordinación clara entre el Ministerio de Defensa, el Ministerio del Interior, el MINTEL y demás entidades competentes, a fin de consolidar una política unificada de protección digital y cultural.
Sr. Michel Santana, Especialista en Ciberseguridad	El compareciente, ingeniero en informática con experiencia en instituciones públicas y privadas del país, expuso sus observaciones al proyecto de ley, estructuradas en tres ejes principales: transparencia, sostenibilidad presupuestaria y desarrollo territorial y talento local. En cuanto al eje de transparencia, propuso incorporar la obligación de publicar informes anuales o habilitar una plataforma digital que refleje estadísticas sobre ciberataques, auditorías e inversiones, así como niveles de madurez institucional. Señaló que esta medida fomentaría la confianza ciudadana y permitiría a las personas conocer si sus datos han sido vulnerados, a fin de adoptar medidas preventivas. Respecto al eje de sostenibilidad presupuestaria, planteó que las instituciones públicas destinen un porcentaje fijo de su presupuesto a capacitación, certificaciones, auditorías y consultorías especializadas en ciberseguridad. Consideró que esto fortalecería las acciones preventivas y la preparación técnica frente a posibles vulnerabilidades. En relación con el eje de desarrollo territorial y talento local, sugirió que las entidades públicas, en coordinación con el MINTEL, los gobiernos autónomos descentralizados y las universidades, organicen concursos, simulacros y laboratorios de ciberseguridad. Indicó que estas actividades contribuirían a fortalecer la cultura de seguridad digital, detectar talento técnico nacional e impulsar la cooperación público-privada y la innovación tecnológica. Finalmente, destacó que estas propuestas permitirían fortalecer la resiliencia institucional, descentralizar la política de ciberseguridad, incentivar el talento juvenil y promover la rendición de cuentas sobre los incidentes cibernéticos. Concluyó señalando que la seguridad digital debe concebirse como una política participativa, transparente y sostenida, en la que los gobiernos autónomos descentralizados desempeñen un papel activo en la protección del ecosistema digital del Estado ecuatoriano.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
Sesión Ordinaria Nro. 44 Fecha: jueves, 30 de octubre de 2025 Modalidad: Semipresencial Link: https://www.facebook.com/100079593587259/videos/815497984535023 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Sr. Patricio Quevedo, Apoderado especial y Procurador Judicial de la Compañía Starlink	El Sr. Patricio Quevedo Vergara, apoderado especial y procurador judicial de la compañía Starlink Ecuador S. A., subsidiaria de Starlink y, a su vez, de SpaceX (Estados Unidos), inició su participación señalando que el Ecuador se encuentra en un proceso crucial de discusión de una Ley de Ciberseguridad, la cual calificó como "hipernecesaria" para el país. Destacó que, tradicionalmente, en Ecuador se ha concebido la seguridad como un ámbito puramente físico, sin considerar con suficiente profundidad la dimensión digital y tecnológica, lo cual constituye a su juicio un error que debe superarse. Subrayó que la infraestructura tecnológica constituye una condición esencial para garantizar la ciberseguridad, por lo que propuso que el proyecto de ley en debate sea aprovechado como una oportunidad estratégica para impulsar el desarrollo y modernización de la infraestructura crítica digital del país. Explicó que dicha infraestructura incluye todos aquellos sistemas cuya alteración o interrupción podría comprometer las funciones esenciales del Estado, particularmente en el ámbito de la seguridad nacional. En ese contexto, planteó la necesidad de reconocer e integrar la tecnología satelital de órbita baja (LEO) dentro del marco de infraestructura crítica digital. Explicó que el Internet satelital LEO ofrece una alternativa de conectividad más económica, resiliente y segura que las redes tradicionales por cable o fibra óptica, ya que su funcionamiento no depende de infraestructura física terrestre. Señaló que esta tecnología, basada en una constelación de más de 8.000 satélites (que se prevé aumentará a 20.000), proporciona cobertura global, baja latencia, alta velocidad y resistencia ante fallas o sabotajes. Resaltó además que, en caso de desastres naturales o ataques cibernéticos, esta red garantizaría la continuidad operativa y la soberanía tecnológica del país, al asegurar la comunicación entre las Fuerzas Armadas, la Policía Nacional, el ECU-911, hospitales, instituciones educativas y demás organismos del Estado.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	También identificó una brecha regulatoria en Ecuador, ya que actualmente no existe un título habilitante específico para la prestación de servicios de Internet satelital LEO. Explicó que los requisitos vigentes para los servicios satelitales tradicionales (geoestacionarios) resultan obsoletos e incompatibles con esta nueva tecnología, generando barreras legales y económicas que impiden su implementación en el país. Propuso, por tanto, que la Ley de Ciberseguridad incorpore una disposición reformatoria a la Ley Orgánica de Telecomunicaciones, a fin de incluir y regular expresamente las tecnologías satelitales de órbita baja como infraestructura crítica digital, con el propósito de fortalecer la resiliencia operativa, la continuidad del Estado y la ciberdefensa nacional.
Sra. Andrea Tenesaca, Especialista en Ciberseguridad y Seguridad de la Información	Durante su intervención, la especialista en ciberseguridad valoró positivamente el Proyecto de Ley para el Fortalecimiento de la Ciberseguridad, al considerar que constituye un avance normativo significativo, pues deja de ser meramente declarativo como la Ley de Transformación Digital para establecer obligaciones concretas tanto en el ámbito público como privado. No obstante, señaló la necesidad de precisar competencias, fortalecer la coordinación interinstitucional y establecer un régimen sancionador claro. Destacó que el artículo 1 acierta al definir la ciberseguridad, aunque propuso incluir una cláusula de prevalencia que garantice su complementariedad con las normas existentes y distinguir entre seguridad digital y ciberseguridad, esta última enfocada en la gestión técnica y operativa de riesgos. En cuanto al artículo 20, sugirió incorporar los principios de proporcionalidad y minimización de riesgos, mientras que en el 20-B planteó crear un mecanismo de “safe harbor” que incentive la notificación oportuna de incidentes sin sanciones, fortaleciendo la transparencia y la cooperación con el CSIRT Nacional. Respecto al artículo 20-E, recomendó formalizar la coordinación con la Autoridad de Protección de Datos Personales mediante protocolos obligatorios y seguros. Sobre la infraestructura crítica digital, pidió definir criterios de clasificación por sectores estratégicos y vincularlos al Sistema Nacional de Gestión de Riesgos, para asegurar una respuesta efectiva ante amenazas.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	En relación con el artículo 20-J, consideró adecuado exigir que los sistemas de seguridad del sector privado cumplan con estándares internacionales auditables, y en el artículo 24 propuso establecer un mecanismo de cooperación formal entre ARCOTEL y el ente rector de ciberseguridad. Finalmente, sobre la cooperación internacional (art. 20-K), planteó dividirla entre asistencia técnica y jurídica, respetando la soberanía y el debido proceso. Concluyó que el proyecto representa un paso decisivo hacia una política nacional integral de ciberseguridad, siempre que se garantice la formación continua del talento humano, la adopción de estándares internacionales y un financiamiento sostenido que permita fortalecer la protección de la infraestructura digital del país.
Sr. Julio Rosas, **Experto en Ciberseguridad**	El especialista en infraestructura de servidores, redes y comunicaciones, inició su intervención subrayando que "no hay transformación digital sin ciberseguridad", enfatizando que el proyecto de ley constituye un avance integral y estructural para el país, al reconocer a la ciberseguridad como un pilar esencial de la transformación digital. En primer lugar, destacó que la definición de ciberseguridad incluida en el proyecto es adecuada, aunque propuso sustituir el término "medios digitales" por "activos digitales", ya que este último abarca información, sistemas e infraestructuras donde realmente se aplican las políticas de seguridad. Explicó que "medio digital" alude más bien a canales de comunicación o plataformas, mientras que el concepto de activo digital refleja de manera más precisa el ámbito técnico de la ciberseguridad. Asimismo, observó que la infraestructura crítica digital, aunque mencionada en la exposición de motivos y en el artículo 2 del proyecto, no cuenta con una definición expresa en el artículo 5, por lo que recomendó incorporarla para otorgarle sustento jurídico y claridad conceptual. En relación con el artículo 20-J, señaló que este hace referencia a los "proveedores de servicios esenciales", sin definir claramente qué se entiende por tales. Propuso que se establezca una clasificación detallada de los servicios esenciales y críticos para el sector privado, con el fin de evitar ambigüedades o conflictos en la aplicación de sanciones y en los contratos que el Estado mantenga con proveedores tecnológicos.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	Respecto al artículo 20-G, consideró necesario incluir un listado mínimo de ministerios e instituciones clave que conformen el Comité de Ciberseguridad, a fin de dotar de mayor seguridad jurídica y operatividad a su accionar. Sostuvo que, además del Ministerio de Telecomunicaciones, deberían integrarlo entidades como ARCOTEL y otros organismos con competencia tecnológica y de defensa digital. Finalmente, comentó sobre la disposición transitoria del proyecto, que establece una fase preventiva y no sancionatoria durante el periodo de emisión de la normativa técnica de fiscalización. A su criterio, este enfoque de transición gradual es positivo, siempre que se aclare que las sanciones solo aplicarán ante incumplimientos graves o deliberados que afecten servicios esenciales, evitando así incertidumbre normativa. Concluyó que el texto constituye un avance sustancial hacia una política nacional de ciberseguridad sólida, siempre que se precisen las definiciones, se delimiten responsabilidades institucionales y se garantice una implementación progresiva y coordinada del marco regulatorio.
Sr. Luis Alberto Urgiles, Experto en Ciberseguridad	El Ing. Luis Alberto Urgilés, magíster en DevOps y especialista en cloud computing, señaló que el ciberespacio debe considerarse el quinto dominio estratégico junto con la tierra, el mar, el aire y el espacio, y que su protección es esencial para la soberanía nacional. Indicó que el Ecuador enfrenta amenazas que requieren un enfoque integral, por lo que el Proyecto de Ley de Fortalecimiento de la Ciberseguridad debe abordar tanto la ciberseguridad como la ciberdefensa. Propuso ampliar el objeto de la ley para reconocer la transformación digital como pilar de la seguridad integral y reformar el Comité Nacional de Ciberseguridad para incluir delegados del Comando Conjunto de las Fuerzas Armadas y del Centro de Inteligencia Estratégica, fortaleciendo la coordinación entre los distintos dominios. Sugirió reformar la composición del Comité Nacional de Ciberseguridad, creado en el artículo 20-L del proyecto, para que incluya de manera permanente a delegados de alto nivel del Comando Conjunto de las Fuerzas Armadas y del Centro de Inteligencia Estratégica, junto con el Ministerio de Telecomunicaciones (MINTEL). Consideró

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	que esta integración es indispensable para coordinar las acciones en los cinco ejes: tierra, mar, aire, espacio y ciberespacio. Respecto a la definición de infraestructura crítica, indicó que el Catálogo Nacional de Infraestructura previsto en el artículo 20-HDB debe concebirse como una infraestructura crítica y estratégica multidominio. Sugirió que se incluyan no solo los sistemas informáticos civiles, sino también los sistemas de control industrial, los sistemas de mando y control militares, los de tráfico aéreo, los portuarios, los telepuertos y las redes de videovigilancia administradas por los gobiernos autónomos descentralizados (GAD). En su cuarta observación, planteó establecer un mandato de interoperabilidad técnica que cree un puente formal entre el ECUSERT, bajo el MINTEL, y el Comando de Ciberdefensa. Explicó que este vínculo permitiría compartir inteligencia de amenazas en tiempo real, de modo que una vulnerabilidad detectada en el ámbito civil por ejemplo, en un banco o industria con dispositivos LoT pueda ser analizada de inmediato por su posible impacto en el ámbito militar o en infraestructuras críticas. Advirtió que, con el desarrollo de tecnologías como la industria LoT y la red 5G, el Ecuador se enfrenta tanto a nuevas oportunidades de crecimiento como a riesgos crecientes de ciberataques y delitos informáticos. Por ello, consideró fundamental que la ley contemple el combate al software pirata y al consumo ilegal de contenidos digitales, así como la integración de todos los actores que intervienen en la seguridad digital, incluyendo los sistemas de videovigilancia públicos y privados.
Sr. Ola Bini, **Experto en Ciberseguridad**	El representante de la empresa Seguridad Digital EC destacó la necesidad de que el Ecuador avance hacia una soberanía digital, advirtiendo que la dependencia tecnológica de empresas extranjeras como Google, Palantir o Starlink pone en riesgo la autonomía y seguridad nacional, al centralizar los datos y decisiones fuera del país. Señaló que la ley propuesta constituye un avance positivo, pero que debe fortalecerse para garantizar que el desarrollo digital esté basado en infraestructura y conocimiento local. Cuestionó el modelo chino de ciberseguridad, señalando que el “gran cortafuegos” sirve principalmente para la censura y no garantiza verdadera protección, ya que elimina el cifrado y vulnera la privacidad. Desde esa

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	perspectiva, insistió en que no se puede tener ciberseguridad real si existen puertas traseras o mecanismos de vigilancia masiva. Entre sus recomendaciones principales, propuso la implementación de una cédula digital nacional que permita centralizar la autenticación de los servicios públicos con mecanismos de multifactor de seguridad, siguiendo modelos como los de Suecia o Estonia. También planteó que la ley deje de lado la neutralidad tecnológica y priorice el uso de software libre, para fomentar la transparencia, la participación ciudadana y el desarrollo de capacidades técnicas dentro del país. Asimismo, subrayó la importancia de incorporar en la legislación una cláusula de "Safe Harbor" que proteja a los investigadores de ciberseguridad que reporten vulnerabilidades de buena fe, tal como ya ocurre en la Unión Europea y otros países. Explicó que actualmente, en Ecuador, quienes intentan alertar sobre fallos de seguridad carecen de respaldo legal, lo que desincentiva la cooperación y debilita la defensa digital nacional. Advirtió también sobre la vulnerabilidad de los algoritmos actuales de firma digital, que podrían quedar obsoletos ante el avance de la computación cuántica, por lo que sugirió actualizarlos de forma preventiva. Finalmente, recomendó que la ley incluya la obligación de realizar un informe post-incidente o de lecciones aprendidas tras cada evento de seguridad, para fortalecer la respuesta institucional y la mejora continua. Concluyó señalando que Ecuador debe apostar por la educación en ciberseguridad, la colaboración público-privada y la protección total de los sistemas sin puertas traseras, ya que la evidencia internacional demuestra que estas vulneran más de lo que protegen.
Sra. Sara Zambrano, Experta en Ciberseguridad	La representante del Centro de Autonomía Digital inició su intervención destacando la necesidad de reconocer que el proceso de digitalización, aunque genera oportunidades para optimizar el servicio público, también produce exclusión. Señaló que el Ecuador avanza en conectividad, pero deja atrás a sectores rurales y poblaciones sin acceso adecuado a las tecnologías. Explicó que su organización aborda estos temas desde una perspectiva de derechos humanos digitales, subrayando la urgencia de contar con una ley específica de ciberseguridad, independiente de la reforma a la Ley de Transformación Digital y Audiovisual, pues el

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
	tratamiento actual resulta limitado para abordar el tema de manera integral. Observó que la vulneración de sistemas no ocurre únicamente por ataques, sino también por la falta de medidas preventivas, lo que expone la información de los ciudadanos. En cuanto a la cooperación internacional, mencionó que si bien es necesaria, el Convenio de Budapest, la Convención de la ONU sobre Ciberdelincuencia y su segundo protocolo adicional presentan aspectos que podrían afectar derechos como la privacidad y la protección de datos personales, especialmente al permitir intercambios de información que podrían comprometer el cifrado de extremo a extremo. Asimismo, recordó casos como NovaStrar (2019) y los ataques a la CNT, en los que se evidenció falta de transparencia y ausencia de sanciones, destacando la importancia de crear un Catálogo Nacional de Infraestructura Crítica Digital y fortalecer los mecanismos de rendición de cuentas ante incidentes. Cuestionó cómo se integrará esta normativa con la Política Nacional de Ciberseguridad, expresando dudas sobre la capacidad del Comité Nacional de Ciberseguridad, dada la alta tasa de ataques que sufre el país. Indicó también que, aunque la ley propone auditorías de seguridad, debería contemplar las actividades ofensivas controladas como herramienta legítima de verificación, y exigir que las instituciones informen con transparencia sobre los incidentes. Planteó la necesidad de establecer medidas de compensación para los ciudadanos afectados y sanciones efectivas para las entidades responsables, señalando que la falta de criterios claros para definir qué es un “incidente relevante” puede limitar la eficacia del sistema de reporte. Mencionó además las limitaciones operativas del EcuCERT, que cuenta con pocos funcionarios y tiempos de respuesta deficientes, lo que obliga a recurrir a canales extraordinarios. En cuanto a los Gobiernos Autónomos Descentralizados (GADs), consideró esencial que reciban recursos para implementar infraestructura y contratar especialistas en ciberseguridad. Finalmente, advirtió sobre el riesgo de centralizar la información nacional en plataformas internacionales como Google o Starlink, lo que implica una pérdida de soberanía digital y falta de control sobre los datos.

Observaciones recibidas en comisión general	
Participante en comisión general	**Resumen de observaciones**
Sesión Ordinaria Nro. 046 Fecha: 19 de noviembre de 2025 Modalidad: Presencial Link: https://www.facebook.com/ComisionSoberaniaAN/videos/1849045242423760 Nota aclaratoria: El enlace referido ya no se encuentra disponible en Facebook debido a sus políticas internas. Sin embargo, el contenido íntegro de la sesión consta en las actas respectivas, accesibles mediante el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing	
Mgs. Paul Palate, Subsecretario de Gobierno Electrónico y Registro Civil del Ministerio de Telecomunicaciones y de la Sociedad de la Información	El Subsecretario de Gobierno Electrónico y Registro Civil del Ministerio de Telecomunicaciones y de la Sociedad de la Información, señaló que, para el Ministerio, resulta significativo que el país avance en la discusión de temas que hoy son prioritarios a escala global. Indicó que la comisión ha convocado a todos los actores relevantes del ecosistema de ciberseguridad y que, como resultado de ese trabajo técnico, el ministerio se encuentra afinando únicamente aspectos de detalle dentro de la propuesta presentada. Destacó que la iniciativa constituye una oportunidad para fortalecer la Ley de Transformación Digital y Audiovisual y la Ley Orgánica de Telecomunicaciones, a fin de lograr un marco normativo más coherente entre ambas. Entre las observaciones planteadas, mencionó la necesidad de revisar el nombre de la reforma, para que abarque también la Ley de Telecomunicaciones. Asimismo, respecto del artículo 1, literal b, sugirió ampliar su alcance tomando como referencia el artículo 225 de la Constitución, con el propósito de incluir sectores que no han sido considerados, como las empresas públicas. Agregó que, en el artículo 4, sería pertinente ajustar ciertas definiciones para alinearlas con el objetivo general de la reforma. Señaló que no existen observaciones de fondo adicionales, excepto en lo relativo al régimen sancionador, para lo cual propuso reformar la Ley de Telecomunicaciones y designar a la Agencia de Regulación y Control como entidad competente en esta materia, en concordancia con el régimen administrativo sancionador establecido en el COA.

2.4. Observaciones remitidas durante el proceso de socialización.

La Comisión conoció y analizó dichas observaciones, cuya documentación integra se encuentra disponible en el siguiente enlace:

https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing.

A continuación, se detallan las observaciones presentadas por las y los asambleístas:

2.4.1. Observaciones de asambleístas.

Nro.	ASAMBLEÍSTA	ASPECTOS OBSERVADOS
1	**As. Lenin Alejandro Lara Pérez**	El asambleísta Lenin Alejandro Lara Pérez compareció en Comisión General, en Sesión Nro. 20, de fecha 18 de agosto de 2025, interviniendo sobre los aspectos contenidos en el proyecto de ley. En relación con las observaciones remitidas por escrito mediante Memorando Nro. AN-LPLA-2025-0045-M, de 6 de agosto de 2025, se deja constancia de que su contenido guarda correspondencia sustancial con los criterios expuestos durante su comparecencia; por tal razón, y a fin de evitar duplicidad de información, se incorpora la documentación remitida de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1AdIl9vkp8QGdMccvzj4Z6T8FoDpkmI8a
2	**As. Inés Margarita Alarcón Bueno**	• **Artículo 20 -L** Las NIST no son estándares Internacionales. NIST significa “National Institute of Standars and Technology” de los Estados Unidos; sería como nuestro INEN. Es decir, se aplicarían estándares de un país, no estándares internacionales, y esos estándares están hecho bajo las condiciones políticas y geopolíticas del país y se usan principalmente en compras públicas. De incluirse estándares de un país, sería adecuado establecer de algunos, para no generar un sesgo. El NIST cybersecurity CSF menciona: “El Marco de Seguridad Cibernética del NIST (CSF) 2.0 proporciona directrices a la industria, agencias gubernamentales y otras organizaciones para gestionar los riesgos de seguridad cibernética. El CSF no especifica cómo se deben lograr los resultados. Más bien, establece enlaces a recursos en línea que proporcionan orientación adicional sobre prácticas y controles que se podrían utilizar para lograr esos resultados. La confianza mutua en la comunidad internacional se basa en un marco de orientación más fiable a nivel mundial que el de un solo país (NIST CSF). Evita que las empresas se enfrenten a una segunda certificación costosa en el momento de la exportación por no cumplir con requisitos como la norma ISO 27001. Hay que asegurar que las medidas de seguridad sean institucionalizadas y continuas (el núcleo de la norma ISO 27001) y no solo improvisadas con una guía flexible (al estilo de CSF del NIST).

		Garantiza que la comunicación y la colaboración con socios internacionales se realicen utilizando un conjunto de estándares reconocidos a nivel mundial en la cooperación técnica, el intercambio de información sobre amenazas de ciberseguridad y las auditorías de seguridad de empresas multinacionales. Texto Sugerido: Artículo 20-L.- Responsabilidades del sector privado en materia de ciberseguridad. - Los prestadores de servicios digitales, proveedores de servicios esenciales y operadores de infraestructura crítica deberán: a) Implementar sistemas de gestión de seguridad de la información basados en estándares internacionales. • **Artículo 20-B,1)** Mejorar la redacción del principio de neutralidad tecnológico. Texto sugerido: l) Neutralidad tecnológica. La adopción de marcos normativos y soluciones de ciberseguridad debe realizarse sin favorecer tecnologías, marcas o proveedores específicos, promoviendo la interoperabilidad, la innovación abierta y la adaptabilidad tecnológica. • **Disposición Transitoria Cuarta** El ciberdelito y la ciberseguridad son conceptos totalmente diferentes. Este proyecto es la mejora de la "Ley Orgánica de Ciberseguridad", mientras que el Convenio de Budapest está relacionado con el ciberdelito; se centran en temas distintos y no deben mezclarse. La Convención de Budapest no se ha actualizado durante muchos años y puede que ya esté obsoleta. La nueva tendencia es la Convención de las Naciones Unidas contra la Ciberdelincuencia, que la Vicepresidenta acabo de firmar en Vietnam el 25 de octubre de 2025. Texto sugerido: Cuarta. - El ente rector en materia de transformación digital, 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.
3	**As. Andrés Felipe Castillo Maldonado**	Las telecomunicaciones son el soporte material de todos los servicios esenciales modernos: sistemas de salud, energía, banca, gobierno electrónico, plataformas educativas, transporte inteligente, y seguridad pública. En las comparecencias recibidas por esta Comisión se ha enfatizado que cualquier avance en ciberseguridad pierde eficacia si el marco regulatorio del sector telecomunicaciones no incluye obligaciones claras de seguridad, continuidad operativa, gestión de incidentes y cooperación con el ente rector.

		Dado que la amenaza digital sobre redes y servicios ha crecido exponencialmente incluyendo ataques DDoS, compromisos de routers, secuestro de tráfico, interrupción de enlaces internacionales y manipulación de equipos de red , resulta imprescindible modernizar la Ley Orgánica de Telecomunicaciones para armonizarla con los principios de la nueva arquitectura nacional de ciberseguridad. Texto propuesto: "Art. 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), seguirá 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." "Artículo […].- Agréguese a continuación de la disposición transitoria novena la siguiente: Décima. En treinta (30) días improrrogables desde la publicación de esta reforma, la Agencia de Regulación y Control de las Telecomunicaciones deberá incorporar al Reglamento para Otorgar Títulos Habilitantes para Servicios del Régimen General de Telecomunicaciones y Frecuencias del Espectro Radioeléctrico el título habilitante de Registro de Servicio de Provisión de Acceso a Internet Satelital de Órbita Baja. En la definición de dicho título habilitante deberá considerarse el régimen especial de tarifas por el uso y explotación del espectro radioeléctrico del artículo 108 de esta Ley, así como los elementos diferenciadores de la tecnología relacionados a la disponibilidad de frecuencias adicionales sujetas a concesión."
4	**As. Camila Anahí Cueva Toro**	Los incidentes documentados en materia de manipulación de radares, adulteración de calibraciones, ataques a sistemas de pesaje y fallas inducidas en plataformas de control vehicular, demuestra que la infraestructura de tránsito se ha convertido en un vector crítico de riesgo para la seguridad integral del país. La progresiva automatización de los mecanismos de captación de infracciones, la dependencia tecnológica en procesos de control, y la creciente exposición de sistemas de movilidad a riesgos digitales requieren que la legislación de tránsito incorpore estándares que garanticen integridad técnica, transparencia y resiliencia. Por ello, y en atención a la necesidad de proteger recursos públicos, evitar incentivos perversos en la contratación de equipos tecnológicos, fortalecer la confianza ciudadana y asegurar la continuidad operativa de la infraestructura vial en escenarios de riesgo, se propone la incorporación de las siguientes reformas a la Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial. Texto Propuesto: "Artículo […].- Realícense las siguientes reformas: Añádase el siguiente literal, después del d), en el artículo 30.3a: "e) Con la finalidad de salvaguardar los recursos públicos, y evitar mecanismos atentatorios a la integridad pública, cualquier tipo de contrato, acuerdo, convenio, asociación o alianza con una persona natural o jurídica de derecho privado en relación con los medios tecnológicos para captar infracciones de tránsito, solo puede tener como objeto el pago de los equipos tecnológicos y el servicio de mantenimiento y puesta en marcha de los mismos. La contraprestación en los contratos, acuerdos, convenios, asociación o alianza no puede estar condicionada a los valores que se recauden por las multas de las infracciones detectadas por los medios tecnológicos." 2. Añádase el siguiente inciso en el artículo 64-B: "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." Disposición Transitoria.- 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).”
5	**As. Gema Karolina Dueñas Palma**	A fin de fortalecer el proyecto, se realiza una propuesta en lo relativo a reformas que podrían incorporarse a la Ley Orgánica de Educación Intercultural (LOEI). La evidencia presentada ante esta Comisión, así como los criterios expresados por diversos expertos nacionales e internacionales, coinciden en señalar que la ciberseguridad no es únicamente un asunto tecnológico o institucional, sino también - y sobre todo - un desafío humano y formativo. De ahí la necesidad de integrar, desde el sistema educativo, una base sólida que prepare a niños, adolescentes, familias y docentes para reconocer riesgos, adoptar buenas prácticas y desarrollar competencias digitales que permitan reducir algún ataque nacional. Por este motivo se considera indispensable que la LOEI incorpore, de forma expresa, la educación en ciberseguridad como un eje estructural del sistema educativo, incluyendo contenidos curriculares obligatorios sobre higiene digital, ciudadanía digital, privacidad, manejo seguro de redes, prevención del acoso y fraude en entornos virtuales, ética digital y pensamiento crítico frente a la desinformación. Asimismo, es necesario que la LOEI garantice la formación docente en competencias digitales avanzadas, asegurando que las y los maestros cuenten con herramientas para identificar riesgos, orientar a sus estudiantes y gestionar adecuadamente incidentes que afecten a la comunidad educativa. Esta reforma también debería contemplar la creación de protocolos mínimos para la gestión de incidentes de seguridad en instituciones educativas, así como lineamientos sobre el uso seguro de plataformas, la protección de datos de estudiantes y docentes, y la responsabilidad de las instituciones para promover entornos digitales confiables. Es igualmente importante que la LOEI facilite la articulación del sistema educativo con el Sistema Nacional de Ciberseguridad, de modo que exista una coordinación efectiva para la prevención, respuesta y acompañamiento en situaciones que involucren amenazas digitales que afecten a menores de edad. Por último, la reforma debería incluir el fortalecimiento de la alfabetización digital de las familias y la consolidación de una cultura nacional de seguridad digital desde edades tempranas, considerando que gran parte de la vulnerabilidad del país se origina en prácticas inseguras reproducidas en el hogar y en la escuela. Estas reformas, aunque no requieren un desarrollo normativo extenso dentro de la ley de ciberseguridad, sí resultan imprescindibles para asegurar que el esfuerzo legislativo sea coherente, integral y sostenible en el tiempo.

		La LOC, por su naturaleza y alcance, es una herramienta estratégica para asegurar que los contenidos de interés público lleguen a la población de manera sostenida. Integrar la seguridad digital entre los contenidos de transmisión obligatoria permite alcanzar zonas remotas, audiencias vulnerables y grupos sociales que no participan activamente en programas de capacitación tecnológica. Esta medida no implica carga económica adicional para los medios de comunicación y se enmarca plenamente en su función social, especialmente cuando se trata de educación, cultura, salubridad y derechos. La ciberseguridad es hoy una dimensión de los derechos ciudadanos y, por tanto, de interés público nacional. Texto Propuesto: "Sustitución del literal c) del artículo 74 de la Ley Orgánica de Comunicación. "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." De igual forma considera incorporar al texto final del proyecto de Ley Orgánica de Ciberseguridad una disposición que regule expresamente el proceso de implementación interna de las obligaciones del ente rector, con el fin de dotar de realismo institucional, coherencia operativa y sostenibilidad al modelo de gobernanza previsto en la ley, sin que ello se interprete como una suspensión de la exigibilidad normativa ni como una alteración de los plazos y efectos previstos en las disposiciones transitorias del proyecto. Texto propuesto: "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."
6	**As. Mario Amado Zambrano Vera**	Durante las comparecencias recibidas por esta Comisión, uno de los expertos invitados, Ola Bini, expuso de manera clara la necesidad de que el Estado ecuatoriano se prepare frente a las amenazas emergentes derivadas del avance exponencial de la computación cuántica, las cuales, según estándares internacionales (NIST, ENISA, ISO/IEC), tienen el potencial de comprometer los mecanismos criptográficos tradicionales utilizados en la actualidad. En su intervención, el experto destacó que varias infraestructuras críticas del Estado —incluyendo la firma digital, los sistemas de autenticación y los protocolos criptográficos utilizados para proteger datos y servicios esenciales— podrían volverse vulnerables en un futuro no lejano, razón por la cual los países están

		iniciando procesos de transición hacia esquemas resilientes y criptografía post-cuántica. En consecuencia, se propone fortalecer el proyecto de ley mediante la incorporación explícita de disposiciones normativas que permitan anticipar la transición tecnológica y dotar de flexibilidad al ente rector para emitir lineamientos técnicos cuando corresponda. Texto Propuesto: "a) Incorporación del principio de adaptabilidad tecnológica (computación cuántica) Lugar sugerido: Artículo 20-B — Principios de ciberseguridad. 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. b) Atribución complementaria para el ente rector en materia criptográfica Lugar sugerido: Artículo 7-A — Atribuciones del ente rector. g) 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." Así mismo varios expertos plantearon la necesidad de incorporar y regular pruebas controladas de seguridad. Ecuador enfrenta un déficit crítico de: investigadores de vulnerabilidades, pruebas sistemáticas de seguridad, cultura de divulgación responsable de fallas, y mecanismos institucionales para permitir pruebas de penetración sin temor a persecución penal injustificada. En la actualidad, el ordenamiento jurídico ecuatoriano no distingue claramente entre: un "agente malicioso", y un "investigador o auditor de seguridad que actúa de buena fe". La ausencia de distinción crea un efecto inhibidor que desalienta la investigación independiente, impide la detección temprana de vulnerabilidades, incentiva la ocultación de fallas, aumenta la superficie de ataque nacional, y coloca al país en desventaja respecto a estándares internacionales, que ya cuentan con esquemas de este tipo. Por ello, se propone incorporar estos elementos en el proyecto orgánico y, de manera complementaria, realizar una reforma técnica, acotada y constitucionalmente viable al Código Orgánico Integral Penal, que permita: proteger a investigadores que actúan dentro de un protocolo autorizado, modernizar el tipo penal de acceso no autorizado. Texto Propuesto:

		"Artículo […].– Evaluación de vulnerabilidades y hacking ético .- Las entidades públicas, los prestadores de servicios digitales 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) Responsabilidad profesional. Las personas naturales o jurídicas que realicen actividades de hacking ético deberán estar registradas ante el ente rector en materia de ciberseguridad o acreditadas por entidades reconocidas en certificaciones profesionales nacionales o internacionales. 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, los mecanismos de registro y acreditación de profesionales, y las medidas de responsabilidad aplicables en caso de incumplimiento de las condiciones previstas en este artículo." Artículo […].- Al final del artículo 232 del Código Orgánico Integral Penal, 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."
7	**As. María Besibell Mendoza Ibarra**	• **Artículo 2, literal "q"** Con el objeto de evitar una posible interferencia con las competencias de la Contraloría General del Estado. Asimismo, se aclara que son auditorías técnicas, no auditorías financieras o de gestión.

		Texto propuesto: "q. Realizar o coordinar auditorías técnicas de seguridad digital a las entidades del sector público, de conformidad con los lineamientos técnicos y estándares nacionales e internacionales, sin perjuicio de las competencias de la Contraloría General del Estado, organismos de control sectoriales y demás entidades de fiscalización previstas en la Constitución y la ley." • **Artículo 2, literal "t"** La reforma propuesta al literal t) busca que la Política Nacional de Ciberseguridad se formule en coordinación expresa con el Comité Nacional de Ciberseguridad, de modo que este no se perciba como una instancia paralela al ente rector, sino como un órgano de apoyo y articulación estratégica. De esta forma se clasifican los roles y se refuerza la coherencia de la gobernanza de la seguridad como política de Estado. Texto propuesto: "Formular la Política Nacional de Ciberseguridad, articulada con los planes nacionales de desarrollo y con las políticas de defensa, seguridad pública y protección de datos personales, en coordinación con los sectores público, privado, académico y la sociedad civil, y en articulación con el Comité Nacional de Ciberseguridad."
8	**As. Gerardo Eugenio Machado Clavijo**	• **Artículo 1** La reforma fortalece el objeto de la ley al incorporar expresamente la ciberseguridad como eje estructural de la transformación digital. El texto vigente omite la protección y seguridad de los entornos digitales, pese a que estos son fundamentales para garantizar la continuidad de los servicios públicos, la confianza ciudadana y la protección de derechos. La inclusión de los principios de resiliencia, integridad, confidencialidad y disponibilidad alinea la norma con estándares internacionales como ISO 27001 y NIST, y dota de coherencia al nuevo capítulo de ciberseguridad. Texto propuesto: "Artículo 1.- Objeto. La presente ley tiene por objeto normar la transformación digital y audiovisual del Estado y de la sociedad ecuatoriana, así como la gobernanza, protección y seguridad de los entornos digitales, en el marco de una gobernanza digital innovadora, centrada en las personas, en los datos, con enfoque de derechos, y con estándares de ciberseguridad que garanticen la resiliencia, integridad, confidencialidad y disponibilidad de la información y los servicios digitales." • **Artículo 2** La ampliación del ámbito de aplicación permite incluir al sector privado que opera infraestructura crítica o servicios esenciales, actores que hoy cumplen un rol determinante en el ecosistema digital. Limitar la ciberseguridad únicamente al sector público genera vacíos normativos y riesgos sistémicos. La inclusión del

		sector privado se plantea bajo el principio de responsabilidad compartida y con obligaciones diferenciadas, fortaleciendo la gobernanza digital. Texto propuesto: "Artículo 2.- Ámbito de Aplicación. Las disposiciones de esta ley son aplicables a todas las entidades de la Administración Pública Central, Institucional y dependiente de la Función Ejecutiva; a las demás funciones del Estado; a los gobiernos autónomos descentralizados; así como a las personas naturales y jurídicas del sector privado que gestionen infraestructura crítica digital, presten servicios esenciales o actúen como operadores relevantes en el ecosistema digital nacional, en lo relacionado con las disposiciones sobre ciberseguridad contenidas en esta ley" • **Artículo 20-A** Este principio reconoce la necesidad de proteger los datos durante todo su ciclo de vida, no únicamente cuando se encuentran almacenados. Además, integra la protección de los medios físicos y lógicos que intervienen en su tratamiento. Su aplicación proporcional permite adaptar las medidas según la naturaleza del riesgo. Esta visión es coherente con los marcos ISO/IEC 27001, NIST y las mejores prácticas internacionales. Texto propuesto (nuevo literal h) : "h. Protección integral del flujo de datos: La ciberseguridad garantizará la protección continua de los datos en todas sus fases: en reposo, en tránsito y en procesamiento, considerando tanto su contenido como los medios físicos y lógicos que los alojan o transportan. Esta protección se aplicará de forma proporcional al nivel de criticidad del dato y al riesgo que represente su vulneración." • **Artículo 20-M – Protección de Medios Físicos y Lógicos de Almacenamiento y Tránsito de Datos – Nuevo*** Este artículo subsana una omisión relevante del marco normativo: la falta de reconocimiento expreso de los medios físicos y lógicos como objetos de protección prioritaria. Permite al ente rector emitir lineamientos específicos sobre seguridad de hardware, software, redes y entornos físicos, materializando técnicamente el principio de protección integral del flujo de datos. Texto propuesto: "Artículo 20-M.- Protección de medios físicos y lógicos de almacenamiento y tránsito de datos. Los dispositivos, sistemas, redes y plataformas tecnológicas que almacenan, procesan o transmiten datos serán considerados objetos de protección prioritaria dentro del marco de ciberseguridad, en función del tipo de información que manejan. El ente rector establecerá directrices técnicas para garantizar su seguridad física, lógica y ambiental, alineadas con estándares internacionales" • **Artículo 20-N - Activos del Ciberespacio como Objeto de Protección – Nuevo*** La incorporación de este artículo permite definir con precisión qué debe ser protegido dentro del ciberespacio, superando una visión limitada a la

		infraestructura crítica. Se incorpora una concepción integral que incluye software, datos, identidades digitales, algoritmos y talento humano. Esto habilita al ente rector a establecer metodologías de clasificación y priorización de activos en función del riesgo, fortaleciendo la resiliencia digital del Estado y de los sectores estratégicos. Texto propuesto: "Artículo 20-N.- Activos del ciberespacio como objeto de protección. Para efectos de esta ley, se entenderá como activos del ciberespacio a todos los recursos físicos, lógicos, informacionales y humanos que intervienen en la creación, procesamiento, almacenamiento, transmisión o control de datos e información digital. Los activos del ciberespacio comprenden, entre otros: infraestructura tecnológica, software, plataformas, sistemas de comunicación, bases de datos, identidades digitales, recursos humanos especializados y algoritmos. El ente rector establecerá criterios para su clasificación, valoración y protección diferenciada, según su nivel de criticidad y riesgo, en concordancia con estándares internacionales.
9	**As. Jhajaira Estefanía Urresta Guzmán**	• **Artículo 1** Se recomienda ajustar la definición de ciberseguridad a fin de evitar una descripción meramente procedimental ("conjunto de políticas, prácticas, estándares y mecanismos") y reemplazarla por una formulación orientada al resultado, que refleje de forma más directa la finalidad esencial de la ciberseguridad. En ese sentido, se propone enfatizar que la ciberseguridad garantiza la confidencialidad, integridad, disponibilidad y protección de los activos digitales, evitando ambigüedades y asegurando coherencia con los principios reconocidos internacionalmente. Texto propuesto: "**Artículo 1.-** Agréguese al final del artículo 5 lo siguiente: g. Ciberseguridad. Conjunto de políticas, prácticas, controles y herramientas destinados a garantizar la confidencialidad, integridad y disponibilidad y protección de la información procesada, almacenada o transmitida en medios digitales. Para efectos de esta ley, las definiciones técnicas específicas relacionadas con activos de información, vulnerabilidades, riesgos y protocolos serán desarrolladas mediante normativa secundaria expedida por el ente rector." • **Artículo 2** Se recomienda especificar de manera expresa la inclusión de las empresas públicas dentro de los actores involucrados en la formulación de la Política Nacional de Ciberseguridad. Aunque el texto menciona la coordinación con el sector público, la referencia es amplia y puede generar ambigüedad respecto a si las empresas públicas, por su naturaleza jurídica y operativa, están contempladas como actores clave en el desarrollo e implementación de dicha política. Por ello, se sugiere incorporar una mención explícita a las empresas públicas para asegurar su participación institucional y operativa en la política nacional de ciberseguridad.

		Texto propuesto: **“** Artículo 2.- Incorpórese los siguientes literales al artículo 7: t. Formular la Política Nacional de Ciberseguridad, articulada con los planes nacionales de desarrollo, en coordinación con los sectores público, incluidas las empresas públicas, privado, académico y la sociedad civil.” • **Artículo 20-D** Se recomienda precisar la expresión “infraestructura crítica” incorporando el término “digital”, a fin de evitar interpretaciones extensivas que incluyan infraestructura física, estratégica o de otra naturaleza no vinculada directamente al ámbito de la ciberseguridad. La normativa debe asegurar que la coordinación estratégica del ente rector en transformación digital se limite exclusivamente a la **infraestructura crítica digital.** Esta precisión fortalece la técnica legislativa, reduce ambigüedades y garantiza la correcta delimitación competencial entre las entidades rectoras de defensa, seguridad y transformación digital. Texto propuesto: “Se agregue el término “digital” • **Disposición General Segunda** Se recomienda especificar y precisar el término “infraestructura crítica local” incorporando expresamente la referencia a “infraestructura digital crítica local”, debido a que, en el contexto de políticas de ciberseguridad y transformación digital, la omisión del término “digital” puede generar confusión con otras infraestructuras físicas o estratégicas cuya regulación y competencias corresponden a otros sectores del Estado. Al referirse a los gobiernos autónomos descentralizados, la normativa debe delimitar claramente que las medidas se enfocan en la infraestructura digital crítica que gestionan a nivel local, esto es, plataformas municipales, sistemas de servicios públicos digitalizados, catastro, redes internas, infraestructura de datos, entre otros. Texto propuesto: “Se agregue el término “digital”
10	**As. Jahiren Elizabeth Noriega Donoso**	• **Artículo 20-R** Texto propuesto: “Artículo 20-R.- Principios aplicables.- El régimen administrativo sancionador en materia de ciberseguridad se regirá, además de por los principios establecidos en la Constitución y en el Código Orgánico Administrativo, por los principios de legalidad, tipicidad, proporcionalidad, seguridad jurídica, debido proceso, especialidad, complementariedad, cooperación interinstitucional y non bis in ídem.

		Las disposiciones de este Capítulo se aplican en armonía con las competencias y procedimientos de los órganos de regulación, supervisión y control especializados, de conformidad con su normativa sectorial, y con las políticas y lineamientos emitidos por el entero rector en materia de transformación." • **Artículo 20-S** Texto propuesto: "Artículo 20-S.- Sujetos responsables. Serán sujetos responsables administrativamente por el incumplimiento de las obligaciones establecidas en este Título, sin perjuicio de otras responsabilidades a que hubiere lugar: a) Las entidades y organismos del sector público, conforme a su respectivo régimen jurídico, cuando gestionen servicios esenciales o infraestructura crítica digital bajo su administración. Las sanciones que se impongan a estos sujetos tendrán carácter esencialmente correctivo o preventivo, sin perjuicio de las responsabilidades administrativas, civiles o penales de sus autoridades, servidoras y servidores. b) Los prestadores de servicios digitales cuya actividad haya sido clasificada como crítica o esencial en el Catálogo Nacional de Servicios Esenciales e Infraestructura Crítica Digital. 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 que emite el ente rector y la autoridad sectorial competente. 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 lo determine el ente rector." • **Artículo 20-T** Presenta una clasificación muy general y poco desarrollada de las infracciones, sin incorporar criterios técnicos claros ni detallar adecuadamente las conductas que configuran cada nivel de gravedad, lo que limitaba su utilidad para la aplicación normativa. La alternativa de propuesta tiene mayor precisión y profundidad, especificando obligaciones, controles y escenarios de riesgo, y definiendo con claridad las conductas sancionables. Texto propuesto: " Artículo 20-T.– Clasificación de infracciones Las infracciones a las obligaciones en materia de seguridad de la información y ciberseguridad se clasifican en leves, graves y muy graves, atendiendo al nivel de afectación a la confidencialidad, integridad, disponibilidad y trazabilidad de la información; al riesgo sistémico generado; y a la criticidad de los servicios, activos o infraestructuras involucrados.

		1. Infracciones leves Se consideran infracciones leves aquellas que constituyen desviaciones formales de bajo impacto y que no comprometen la operación, continuidad ni el estado de seguridad de los sistemas, tales como: a) Demoras injustificadas en la actualización de políticas, procedimientos o planes de ciberseguridad cuando no exista impacto en servicios ni en la postura de seguridad. b) Omisión de reportes periódicos o de información rutinaria requerida por la autoridad competente, cuando dicha omisión no afecte la capacidad de supervisión ni la detección de riesgos. 2. Infracciones graves Se califican como infracciones graves aquellas que incrementan de forma relevante la superficie de exposición al riesgo, afectan la capacidad de respuesta o comprometen controles esenciales, incluyendo: a) No notificar incidentes de seguridad relevantes dentro de los plazos o canales establecidos, cuando dichos incidentes puedan impactar servicios, usuarios, datos o infraestructura crítica. b) No implementar los controles mínimos obligatorios definidos por la normativa, estándares o modelos de referencia aplicables. c) Obstaculizar controles técnicos, verificaciones, pruebas de ciberseguridad o requerimientos formales de la autoridad competente, afectando la supervisión oportuna. d) Reincidencia en infracciones leves. 3. Infracciones muy graves” • **Artículo 15 – COIP** Al permitir que cualquier responsable pueda autorizar el consentimiento de acceso, se debilita la exclusividad en la toma de decisiones. Esta formulación genera vacíos sobre quién tiene realmente la autoridad y abre la posibilidad de que administradores o técnicos tomen decisiones por su cuenta sin el control adecuado. Solo debe consignarse "titular" porque solo él tiene derecho exclusivo para autorizar accesos al sistema. **Texto propuesto:** Artículo 15.- 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, 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.” • **Sección 3 – Código Orgánico Monetario y Financiero**

		De la Superintendencia de Bancos Art. 62 El numeral 9 del artículo 62 del Libro 3 del COMF exige "Estrictos controles" en banca electrónica, pero esta regla general ya no alcanza frente a amenazas cada vez más complejas, como ransomware, phishing o robo de cuentas. Aunque muchas entidades usan estándares como ISO 27001, cada banco los aplica a su manera, generando brechas de seguridad y dejando al sistema financiero expuesto. Además, la mayoría de fraudes ocurre por ingeniería social, por lo que también es clave fortalecer la información que reciben los usuarios sobre cómo proteger sus datos. Una reforma permitiría establecer estándares mínimos comunes, claros y verificables, alineados con prácticas internacionales. Con reglas uniformes, mejor supervisión y un enfoque preventivo, se reduce el riesgo sistémico, se protege a los usuarios y se fortalece la confianza en la banca electrónica y todo el sistema financiero nacional. La reforma actualiza la norma para enfrentar mejor los riesgos digitales, incorporando estándares internacionales como ISO y NIST, haciendo obligatoria la autenticación multifactor e introduciendo controles claros de cifrado, trazabilidad y monitoreo continuo. También establece, por primera vez, un régimen de notificación temprana de incidentes para que usuarios y autoridades puedan responder con rapidez ante cualquier amenaza. Además, fortalece la información y los derechos del consumidor financiero en materia de seguridad digital, de modo que las personas comprendan cómo protegerse y qué garantías tienen al usar la banca electrónica. Con estas mejoras, el sistema financiero adopta reglas mínimas uniformes que elevan la protección, reducen vulnerabilidades y generan mayor confianza pública. Texto propuesto: "Que se cambie el contenido del numeral 9 del art.62 por el siguiente texto: 9. Disponer a las entidades controladas la adopción, implementación y mantenimiento de un Sistema de Gestión de Ciberseguridad basado en estándares internacionales reconocidos, que garantice la seguridad, integridad, confidencialidad y disponibilidad de los servicios provistos a través de la banca electrónica y cualquier otro canal digital. Para el efecto, deberán cumplir, como mínimo, con: a) Mecanismos de autenticación multifactor aplicables a todas las operaciones electrónicas y a todo acceso remoto de los clientes o usuarios. b) Cifrado obligatorio de la información financiera y de los datos personales en tránsito y en reposo. c) Monitoreo continuo y gestión de riesgos cibernéticos, incluyendo pruebas de penetración, auditorías de seguridad, análisis de vulnerabilidades y control de accesos. d) Notificación obligatoria de incidentes de seguridad a los usuarios afectados y a la Superintendencia, dentro de un plazo máximo de doce (12) horas de haberlos detectado. e) Mecanismos de trazabilidad, registro y conservación segura de eventos electrónicos relacionados con transacciones y accesos.

		Las instituciones financieras deberán informar de manera clara, accesible y previa a sus usuarios y/o clientes sobre las medidas de seguridad aplicables, sus derechos en materia de protección de datos financieros y los cuidados mínimos que deben observar al utilizar claves, contraseñas, datos biométricos y demás factores de autenticación. La Superintendencia queda facultada para emitir normativa técnica adicional, exigir niveles de madurez superiores en materia de ciberseguridad y ordenar la actualización periódica de los controles implementados." • **Artículo 12** El artículo propone incluir en el currículo nacional contenidos sobre seguridad digital, enfocados en el uso responsable de la tecnología, riesgos en línea y buenas prácticas, como ciberacoso y privacidad de la información. Sin embargo, Gabriel Brito, antropólogo digital de la Universidad de Oxford, destaca el "Cártel TikTok", un fenómeno donde organizaciones criminales reclutan a jóvenes vulnerables a través de redes sociales y videojuegos como TikTok, Free Fire y Roblox. Es crucial profundizar en este tema dentro de la educación digital para prevenir el reclutamiento en línea. Gabriel Brito, antropólogo digital e investigador del Instituto del Internet de la Universidad de Oxford, expuso sobre el fenómeno denominado "Cártel TikTok", que evidencia: Problema identificado: Organizaciones criminales normalizan la violencia, difunden su agenda y reclutan principalmente a jóvenes y personas vulnerables a través de redes sociales y videojuegos (TikTok, Free Fire, Roblox). Texto propuesto: "Artículo 12.- 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 la prevención del reclutamiento digital por parte de organizaciones criminales a través de redes sociales, videojuegos y plataformas digitales. 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. d) La identificación de estrategias de captación y reclutamiento criminal en entornos digitales y videojuegos. e) La coordinación con las autoridades competentes en seguridad ciudadana para la prevención del"
11	**As. Adrián Ernesto Castro Pineda**	• Dentro del Artículo 20-H, agréguese el siguiente inciso: *"El CSIRT Nacional realizará ejercicios de ciberseguridad de forma periódica, conforme a las necesidades del ecosistema digital. Su planificación y ejecución se desarrollarán de acuerdo con el reglamento que se dicte para tal efecto."* Se considera necesario agregar este inciso en virtud de que los ejercicios de ciberseguridad son un instrumento técnico necesario en la reforma que nos ocupa la cual ayudará a fortalecer sus capacidades para preservar la seguridad digital como lo realizan en varios países del mundo. La propuesta realizada busca prevención. Sin ejercicios periódicos, el CSIRT actúa solo cuando el daño ya este hecho. Esta propuesta de texto, institucionaliza la prevención operativa, permitiendo anticipar fallas, medir tiempos de respuesta y corregir vulnerabilidades antes de un incidente real. • Dentro del Artículo 20-J, agréguese como literal e) el siguiente texto: *"e) Establecer un responsable de seguridad de la información y ciberseguridad, el cual no podrá pertenecer al área de tecnologías de la información y comunicación de la entidad; tendrá un perfil con formación académica y experiencia en áreas relacionadas con la seguridad de la información y ciberseguridad; cumplirá los demás requisitos determinados en el reglamento general de aplicación de la presente ley."* Lo propuesto en el texto, busca la separación funcional entre las áreas de tecnologías de la información y el responsable de seguridad de la información y ciberseguridad, lo cual responde a principios de control interno, independencia técnica y gestión de riesgos, alineados con estándares y buenas prácticas de gobernanza digital. Esta medida evita conflictos de interés, fortalece la supervisión objetiva de los sistemas críticos del Estado y garantiza decisiones técnicas especializadas, imparciales y orientadas a la protección efectiva de la información pública y los servicios digitales, en estricto cumplimiento del principio de eficiencia, seguridad y responsabilidad en la administración pública. Cabe mencionar que, esto ya se cumple por temas normativos en el sector financiero (normas de la Super de Bancos y SEPS) y el sector público (EGSI V3) por ende se debe considerar el literal propuesto para de esta manera mejorar esta práctica en el sector privado. • En el último inciso del artículo 20-LL, agregar después de la palabra "protección" el término "MONITOREO", siendo el texto propuesto el siguiente:

		"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." La ciberseguridad debe asumirse de manera proactiva como una práctica esencial. En este marco, el monitoreo continuo de los activos digitales es clave para identificar oportunamente amenazas, prevenir incidentes y minimizar el impacto de posibles ataques. La implementación de mecanismos de vigilancia permanente como el monitoreo, objeto de esta observación, fortalece la resiliencia del ecosistema digital y permite detectar comportamientos anómalos o maliciosos antes de que afecten la operación o comprometan la integridad de los sistemas. • En el Artículo 20-R, respecto a las infracciones graves, dentro del numeral 2, se sugiere reemplazar la palabra "omitir" por el término técnico "OCULTAR". Técnicamente, los incidentes no se omiten, sino se ocultan. • En el Capítulo II referente a las Disposiciones Reformatorias, se sugiere agregar la frase "CSIRT NACIONAL" en el artículo 43 de la Ley Orgánica de Protección de Datos Personales, quedando así: *"Art. 43.-Notificación de vulneración de seguridad.-El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y al CSIRT Nacional , 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."* Cuando se creó la Ley Orgánica de Protección de Datos Personales, no existía la Ley Orgánica de Transformación Digital y Audiovisual por consiguiente no existía el equipo de respuesta a incidentes de seguridad informática CSIRT y se reportaba al ARCOTEL. En la actualidad con estos ajustes a la Ley Orgánica de Transformación Digital y Audiovisual se crea el CSIRT NACIONAL con lo cual, se debe notificar a él y no a la Agencia de Regulación y Control de las Telecomunicaciones, ya que éste sólo posee competencias dentro del ámbito de telecomunicaciones.

2.4.2. Observaciones institucionales y ciudadanas.

Nro.	INSTITUCIÓN / ORGANISMO/ ORGANIZACIÓN CIUDADANO	ASPECTOS OBSERVADOS
1	**Cabezas Consultiva Jurídica**	• **Artículo 1** Se sugiere un marco más granular que ofrezca una pormenorización para la identificación de "entidades esenciales" y "entidades importantes", basado en

		la criticidad de los sectores, el tipo de servicio que prestan, su tamaño y el impacto potencial de una interrupción. Sugiere la incorporación de 2 categorías: alta criticidad y criticidad media. Se elabore una normativa específica que complemente la LOPDP y establezca: - Criterios de clasificación sectorial de criticidad cibernética - Regímenes diferenciados de supervisión y reporte de incidentes - Obligación de nombrar Delegados de Ciberseguridad en entidades clave - Protocolos comunes de respuesta a incidentes y resiliencia operativa Este enfoque contribuiría a reducir la fragmentación normativa, cerrar brechas institucionales y reforzar la protección de la infraestructura digital nacional ante el creciente número de ciberataques sufridos en los últimos años. • **Artículo 2** -Se sugiere incluir un mandato explícito para la divulgación coordinada de vulnerabilidades, detallando el rol del EcuCert (o de una entidad designada como coordinador. - La creación o designación de una plataforma o repositorio nacional de vulnerabilidades, quizás interoperable según estándares internacionales, para facilitar la notificación y el intercambio de información sobre vulnerabilidades conocidas y solucionadas. - Requisitos para que los fabricantes de productos con elementos digitales (digital products) implementen políticas de CVD y notifiquen activamente las vulnerabilidades explotadas, a través de una implementación de una "plataforma única de notificación". El proyecto promueve campañas de concientización y formación. Esta directriz debiera fortalecerse instando al compromiso de las organizaciones, y de tal manera, exigiendo que los miembros de los órganos de dirección de las entidades esenciales e importantes asistan a formaciones para adquirir conocimientos y destrezas suficientes para detectar riesgos y evaluar las prácticas de gestión de riesgos. Sin el compromiso de los más altos directivos de las organizaciones públicas o privadas no podemos esperar el éxito de los fines de la Ley: La ley podría contemplar que el ente rector promueva la calificación e implementación en programas de certificación de ciberseguridad voluntarios para productos o servicios digitales, lo que incentivaría la mejora de la seguridad más allá de los requisitos mínimos y facilitaría la confianza en el mercado, como por ejemplo Estándares técnicos y guías de evaluación OWASP ASVS (Application Security Verification Standar), Certificaciones de seguridad de productos por terceros, Certificaciones orientadas a servicios y operaciones. • **Artículo 20 – C** Podría enfatizarse la "divulgación coordinada de vulnerabilidades" (CVD) y la obligación de los fabricantes de establecer políticas para ello. También prever un "CSIRT designado como coordinador" para facilitar la interacción entre notificantes y fabricantes, y una "base de datos ecuatoriana de

		vulnerabilidades" que podría mantener MINTEL, en cuanto ha liderado la estrategia nacional de ciberseguridad. Aunque el proyecto ecuatoriano impone obligaciones a proveedores de servicios digitales, no estaría fuera de lugar enfatizar la evaluación y gestión de los riesgos de ciberseguridad provenientes de la cadena de suministro y la relación con los proveedores, incluidos los componentes de terceros y el software de código abierto. La Ley podría establecer que los fabricantes ejerzan "diligencia debida" al integrar componentes de terceros y especifica a través de normativa secundaria de una "nomenclatura de materiales de los programas informáticos" (SBOM). Se podría considerar la inclusión de un artículo o una disposición en la normativa secundaria que establezca requisitos específicos para la gestión de la seguridad de la cadena de suministro, que desarrolle la obligación de esta ley de realizar una diligencia debida en la selección de proveedores y componentes, y la posible necesidad de una SBOM para ciertos productos o servicios críticos, para mejorar la trazabilidad de vulnerabilidades. • **Artículo 20-G** Podría enfatizarse la "divulgación coordinada de vulnerabilidades" (CVD) y la obligación de los fabricantes de establecer políticas para ello. También prever un "CSIRT designado como coordinador" para facilitar la interacción entre notificantes y fabricantes, y una "base de datos ecuatoriana de vulnerabilidades" que podría mantener MINTEL, en cuanto ha liderado la estrategia nacional de ciberseguridad. • **Artículo 20-I** El proyecto menciona sanciones "de conformidad con la normativa vigente" o "sanciones administrativas conforme a la ley". Sería conveniente, toda vez que existe el principio de legalidad en cualquier tipo de sanción, que las mismas sean incorporadas al texto, basadas en el volumen de negocios o montos fijos para infracciones específicas, asegurando que sean "efectivas, proporcionadas y disuasorias". Sería posible, inclusive, imponer medidas de ejecución más severas, como la suspensión temporal de certificaciones o la prohibición de ejercer funciones de dirección en casos graves. Se sugiere que la normativa técnica especifique un régimen de sanciones más detallado y escalonado para las infracciones en materia de ciberseguridad, incluyendo: - Criterios claros para determinar la gravedad de la infracción. -Topes de multas administrativas que sean lo suficientemente disuasorios, quizás inspirados en un porcentaje del volumen de negocios o montos significativos, adaptados al contexto económico ecuatoriano, como ocurre con la LOPDP. - Consideración de medidas correctivas progresivas antes de la imposición de sanciones máximas que, permitan, también, ir creando cultura de ciberseguridad.
2	**Amazon Web Services**	Los representantes de Amazon Web Services comparecieron ante la Comisión General, en la Sesión Ordinaria Nro. 20, de fecha 18 de agosto de 2025, presentando los aspectos observados sobre el proyecto de ley. En relación con las observaciones remitidas por escrito mediante correo electrónico, se deja

		constancia de que su contenido guarda correspondencia relevante con expuesto en Comisión General; por tal razón, y a fin de mantener la sistematicidad del informe, se incorpora la documentación remitida de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1mA_hHPikO8DQDvbLuoLX4Ykd9W05vXUP
3	**Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL)**	Los representantes de MINTEL comparecieron ante la Comisión General, en la Sesión Ordinaria Nro. 46, de fecha 19 de noviembre de 2025, ocasión en la cual expusieron las observaciones formuladas al proyecto de ley. En relación con las observaciones remitidas por escrito mediante el Oficio Nro. MINTEL-MINTEL-2025-0306-O, de fecha 20 de agosto de 2025, se deja constancia de que su contenido guarda correspondencia relevante con lo expuesto en Comisión General. Asimismo, con fecha 22 de diciembre de 2025, la institución se pronunció sobre nuevas observaciones al proyecto de ley mediante el Oficio N.º MINTEL-MINTEL-2025-0459-O, las cuales complementan y amplían el análisis del proyecto. A fin de mantener la sistematicidad del presente informe, se incorpora de manera íntegra la documentación remitida, disponible para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1YCZncGkB2Cxw-fPAKG2uExf4uMDVT5jZ?usp=drive_link
4	**Superintendencia de Economía Popular y Solidaria**	Los representantes de la SEPS comparecieron ante la Comisión General, en la Sesión Ordinaria Nro. 29, de 16 de septiembre de 2025, presentando los aspectos observados sobre el proyecto de ley. En relación con las observaciones remitidas por escrito mediante el Oficio Nro. SEPS-SGD-2025-24724-OF, de fecha 20 de agosto de 2025, se deja constancia de que su contenido guarda correspondencia relevante con lo expuesto en Comisión General; por tal razón, y a fin de mantener la sistematicidad del informe, se incorpora la documentación remitida de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1Qeq7fgBWIaEp_hlbtoRPKAbdi54d-JnT?usp=drive_link
5	**Lorena Naranjo Godoy, Directora Área de Protección de Datos Personales y Derecho Digital**	La representante compareció ante la Comisión General en la Sesión Ordinaria N.º 28, de fecha 10 de septiembre de 2025, presentando los aspectos observados sobre el proyecto de ley. En relación con las observaciones remitidas por escrito mediante correo electrónico, se deja constancia de que su contenido guarda correspondencia relevante con lo expuesto en Comisión General; por tal razón, y a fin de mantener la sistematicidad del informe, se incorpora la documentación remitida de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1HjW2WEZySg2lIUdxmWn1Gh61by41nhFa?usp=drive_link
6	**Asociación de Bancos del Ecuador (ASOBANCA)**	Los representantes de ASOBANCA comparecieron ante la Comisión General en la Sesión Ordinaria N.º 32, de fecha 24 de septiembre de 2025, presentando los aspectos observados sobre el proyecto de ley. En relación con las

		observaciones remitidas por escrito mediante el Oficio Nro. PE-432-2025-DL462, de fecha 22 de agosto de 2025, se deja constancia de que su contenido guarda correspondencia relevante con lo expuesto en Comisión General; por tal razón, y a fin de mantener la sistematicidad del informe, se incorpora la documentación remitida de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1cTK24C0VfAfMMrhEX3i9Hp0dbmgqR9dd?usp=drive_link
7	**Polo Fabián Iñiguez, Experto en temas de Ciberseguridad**	El especialista compareció ante la Comisión General en la Sesión Ordinaria N.º 26, de fecha 8 de septiembre de 2025, presentando los aspectos observados sobre el proyecto de ley. En relación con las observaciones remitidas por escrito mediante correo electrónico, se deja constancia de que su contenido guarda correspondencia relevante con lo expuesto en Comisión General; por tal razón, y a fin de mantener la sistematicidad del informe, se incorpora la documentación remitida de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1NtJNWA3cJJ6IrgyyxEnOFSwQZ-izoZxJ?usp=drive_link
8	**Asociación Latinoamericana de Internet (ALAI)**	• **Artículo 2** -El literal p, que establece como atribución del ente rector de transformación digital la elaboración, mantenimiento y actualización de un catálogo nacional de infraestructura crítica digital, es importante señalar que el proyecto de Ley no incorpora una definición de “infraestructura crítica digital". Esta ausencia puede generar ambigüedades en la interpretación y aplicación de las obligaciones, particularmente en lo referente a los sujetos que deben ser considerados operadores de dichas infraestructuras. Resulta fundamental que la Ley distinga con claridad entre las responsabilidades de los operadores de infraestructura crítica digital y aquellas de los terceros que proveen soluciones tecnológicas de soporte. Estos últimos como proveedores de servicios de nube, alojamiento de contenido, procesamiento, disponibilidad o seguridad contribuyen al funcionamiento de los sistemas, pero no deben ser considerados operadores de infraestructura crítica digital. Texto propuesto: Se sugiere incorporar en el texto legal definiciones que precisen estos conceptos, tales como: *Infraestructura crítica digital: Es el conjunto de instalaciones físicas, redes, sistemas, plataformas, equipos y demás componentes considerados como activos de información que son necesarios para el funcionamiento continuo de los servicios esenciales, asegurando su disponibilidad, confidencialidad, integridad y resiliencia ante posibles amenazas o interrupciones. Los terceros que ofrezcan servicios de tecnología a los operadores de infraestructura crítica digital, tales como proveedores de servicios de nube, alojamiento de contenido, de alojamiento, procesamiento, disponibilidad, continuidad, seguridad y soporte al servicio digital, o permitan mejorar su desempeño,*

		usabilidad o acceso no son considerados, a su vez, operadores de infraestructura crítica digital para los fines de esta Ley. *Servicio esencial: Servicio indispensable para el cumplimiento de los deberes primordiales del Estado y el funcionamiento de los sectores estratégicos determinados en la Constitución de la República.* Estas precisiones contribuirán a un marco regulatorio más claro, que evite cargas indebidas sobre terceros proveedores de servicios tecnológicos y, al mismo tiempo, garantice la protección adecuada de las infraestructuras críticas digitales y los servicios esenciales que soportan. -El literal q, se sugiere precisar la redacción, ya que no se desarrolla en el texto qué debe entenderse por "auditorías de seguridad digital". El término podría resultar ambiguo y prestarse a distintas interpretaciones. Una alternativa más clara y alineada con las prácticas actuales sería referirse a "ejercicios de ciberseguridad", que incluyen actividades de evaluación, pruebas y validación de la seguridad digital bajo estándares reconocidos. Texto propuesto: *"q. Realizar o coordinar ejercicios de seguridad digital con las entidades del sector público, de conformidad con los lineamientos técnicos y estándares nacionales e internacionales."* - El literal r, propone que el ente rector establezca lineamientos para la gestión de incidentes digitales, promoviendo mecanismos de prevención, detección, respuesta y recuperación en las instituciones públicas. Esta atribución es valiosa, pues contribuye a fortalecer la resiliencia digital del sector público. No obstante, para maximizar su efectividad y garantizar coherencia con marcos ya consolidados a nivel global, sería recomendable que el texto haga referencia explícita a la adopción de buenas prácticas y estándares internacionales (por ejemplo, el NIST Cybersecurity Framework u otros equivalentes). Esto permitiría aprovechar experiencias probadas, asegurar interoperabilidad y generar mayor confianza en la gestión de incidentes. Texto propuesto: *"r. Establecer lineamientos para la gestión de incidentes digitales, promoviendo la implementación de mecanismos de prevención, detección, respuesta y recuperación en las instituciones públicas, siguiendo buenas prácticas y estándares internacionales reconocidos."* • **Artículo 20-A** El concepto de "prestadores de servicios digitales" resulta demasiado amplio y no se encuentra definido en el texto de la Ley, lo que genera riesgos de ambigüedad e inseguridad jurídica. La amplitud de esta expresión podría dar lugar a interpretaciones que extiendan la aplicación de la norma a actores que claramente escapan del ámbito de la misma. En este sentido, se recomienda que la disposición se limite a las entidades públicas y a los operadores de infraestructura crítica digital, conforme a la definición sugerida en el artículo 2. Asimismo, es fundamental que la Ley distinga entre las obligaciones propias de los operadores de infraestructura crítica digital y aquellas que correspondan a terceros proveedores de soluciones tecnológicas (como servicios en la nube, alojamiento de contenido,

		procesamiento o disponibilidad). Estos terceros no deben ser considerados operadores de infraestructura crítica digital, pues cumplen un rol diferente en la cadena de valor. Texto Propuesto: "*Artículo 20-A.- Principios de ciberseguridad. La implementación de políticas, medidas y mecanismos de ciberseguridad por parte de las entidades públicas y los operadores de infraestructura crítica digital se regirá por los siguientes principios: (...)"* • **Artículo 20-C** El artículo, tal como está redactado, introduce el concepto de "prestadores de servicios digitales" en el artículo 20-C, sin ofrecer una definición clara dentro del marco de la ley. Esto genera un ámbito de aplicación demasiado amplio que podría incluir a actores que no deberían estar sujetos a obligaciones de ciberseguridad de este nivel, escapando así del objeto y propósito de la norma. En ese sentido, resulta más preciso y coherente limitar el alcance de la disposición a los operadores de infraestructura crítica digital, en línea con la definición que se recomendó incorporar en el Artículo 2. Esto permite concentrar las obligaciones en quienes efectivamente prestan servicios esenciales para la continuidad del Estado, la economía y la sociedad, evitando cargas regulatorias innecesarias sobre otros actores. Texto propuesto: *"Artículo 20-C.- Responsabilidades de los operadores de infraestructura crítica digital. Los operadores de infraestructura crítica digital deberán adoptar medidas para garantizar la continuidad operativa, la protección contra ciberamenazas y la notificación de incidentes relevantes al ente rector, conforme a la regulación técnica que se expida."* • **Artículo 20-E** Establece la necesidad de coordinar con la Autoridad de Protección de Datos Personales todas aquellas acciones derivadas de la presente ley que tengan incidencia en el tratamiento de datos personales. Asimismo, señala que la elaboración de políticas, protocolos de gestión de incidentes, normas técnicas y cualquier otra medida relacionada con el uso, procesamiento, transferencia o resguardo de datos personales deberá respetar los principios, derechos y garantías previstos en la Ley Orgánica de Protección de Datos Personales, asegurando la no duplicidad de funciones y el respeto a las competencias de cada entidad. Al respecto, consideramos importante reforzar la disposición para que no solo se garantice la coordinación institucional y el respeto de competencias, sino que además se evite expresamente la duplicidad de trámites, reportes o procedimientos sancionatorios que podrían generar cargas innecesarias para los regulados. Esta precisión aporta mayor claridad y seguridad jurídica, previniendo superposiciones normativas y redundancias que afectarían la eficiencia del cumplimiento. Texto Propuesto: *"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, trámites, reportes o procedimientos sancionatorios, así como el respeto a la competencia de cada entidad**.** • **Artículo 20-F** Plantea una coordinación operativa amplia y adecuada entre entidades responsables, pero resulta importante precisar el alcance de algunos conceptos, en particular el de "servicios esenciales". La inclusión de una definición contribuiría a dotar de mayor certeza jurídica y operativa a la implementación de la política de ciberseguridad, evitando interpretaciones dispares por parte de las distintas entidades involucradas. Texto propuesto: Se sugiere incorporar la siguiente definición en el glosario normativo: "*Servicio esencial. – Servicio indispensable para el cumplimiento de los deberes primordiales del Estado y el funcionamiento de los sectores estratégicos determinados en la Constitución de la República."* De esta forma, se refuerza la coherencia normativa y se asegura que las medidas de ciberseguridad protejan efectivamente aquellos servicios cuya interrupción tendría un impacto crítico en el orden público, la seguridad nacional, la salud, la justicia y el desarrollo económico y social del país. • **Artículo 20-G** Establece la obligación de notificar al ente rector en transformación digital cualquier incidente de seguridad digital, aplicable a entidades públicas, prestadores de servicios digitales y operadores de infraestructura crítica digital. Sin embargo, el concepto de "prestadores de servicios digitales" resulta demasiado amplio y no se encuentra definido en el texto legal. Esto puede generar inseguridad jurídica y una extensión desproporcionada del ámbito de aplicación de la norma, abarcando actores que no guardan relación con la gestión de infraestructura crítica ni con las obligaciones propias de las entidades públicas. Adicionalmente, se sugiere ajustar el contenido de las hipótesis de notificación, eliminando aquellas disposiciones que generan redundancias o ambigüedad: ● Eliminar la referencia a la disponibilidad, confidencialidad o integridad de datos personales o institucionales, ya que los incidentes relacionados con datos personales ya se encuentran regulados por la Ley Orgánica de Protección de Datos Personales y, por otro lado, los términos relativos a datos institucionales carecen de precisión técnica.

		● Mantener únicamente la obligación de notificar incidentes que afecten la continuidad operativa de servicios esenciales, eliminando la mención a "servicios críticos", dado que esta categoría no cuenta con definición normativa. ● Suprimir la frase "que pueda escalar o propagarse", debido a su ambigüedad técnica y falta de criterios objetivos, lo que podría dar lugar a interpretaciones subjetivas y notificaciones innecesarias, afectando la eficacia del sistema de gestión de incidentes. ● Se recomienda precisar que el plazo de notificación se cuente a partir del momento en que la entidad tenga un conocimiento razonable del incidente, a fin de evitar reportes innecesarios y garantizar que la obligación se ajuste al principio de proporcionalidad previsto en el apartado 20-A d. Texto Propuesto: *"Artículo 20-G.- Obligación de notificación de incidentes de seguridad digital. Las entidades públicas, y los operadores de infraestructura crítica digital deberán notificar sin dilación indebida al ente rector en transformación digital cualquier incidente de seguridad digital que:* *Afecte la continuidad operativa de servicios esenciales o críticos.* *La notificación deberá realizarse en un plazo máximo de 72 horas desde que la entidad tome conocimiento razonable de su detección, de conformidad con los protocolos que establezca el ente rector. La omisión injustificada será* sancionada de conformidad con la normativa vigente." • **Artículo 20-H** En relación con el Artículo 20-H sobre la clasificación de infraestructura crítica digital, consideramos positivo que se establezcan criterios para su identificación y protección. Sin embargo, sugerimos precisar la definición de infraestructura crítica digital, de manera que se oriente adecuadamente el proceso regulatorio y se eviten ambigüedades. Texto propuesto: "Infraestructura crítica digital. – Es el conjunto de instalaciones físicas, redes, sistemas, plataformas, equipos y demás componentes considerados como activos de información que son necesarios para el funcionamiento continuo de los servicios esenciales, asegurando su disponibilidad, confidencialidad, integridad y resiliencia ante posibles amenazas o interrupciones. Los terceros que ofrezcan servicios de tecnología a los operadores de infraestructura crítica digital, tales como proveedores de servicios de nube, alojamiento de contenido, procesamiento, disponibilidad, continuidad, seguridad y soporte al servicio digital, o que permitan mejorar su desempeño, usabilidad o acceso, no son considerados, a su vez, operadores de infraestructura crítica digital para los fines de esta Ley." Adicionalmente, consideramos que la sensibilidad de los datos procesados no debería ser un criterio para determinar si una infraestructura es crítica. Ecuador ya cuenta con normativa específica para la protección de datos personales, por lo que la inclusión de este factor podría generar redundancias normativas y confusiones en la aplicación de la Ley. En consecuencia, sugerimos eliminar el literal c) del artículo.

		• **Artículo 20-I** El alcance del Artículo 20-I resulta excesivamente amplio y carece de delimitación normativa suficiente. Tal como está planteado, habilita al ente rector a ejercer facultades de fiscalización sobre todo tipo de entidades, incluyendo las privadas, sin establecer criterios claros, procedimientos definidos ni salvaguardas mínimas. Esta amplitud puede generar riesgos de discrecionalidad y eventuales conflictos de competencias con marcos regulatorios ya existentes, como los sectoriales o los relativos a la protección de datos personales. En este sentido, se recomienda precisar el ámbito de aplicación del artículo, limitando expresamente la facultad de fiscalización del ente rector a las entidades públicas sujetas a la ley, con el fin de garantizar coherencia normativa, seguridad jurídica y respeto a las competencias de otras autoridades. Texto Propuesto: *"Artículo 20-I.- Fiscalización y medidas correctivas.- El ente rector podrá realizar acciones de fiscalización técnica a las entidades públicas sujetas a esta ley, a fin de verificar el cumplimiento de las obligaciones en materia de seguridad digital. En caso de incumplimiento, podrá disponer: (...)"* • **Artículo 20-J** En relación con el artículo 20-J, consideramos que la inclusión de las "entidades financieras" resulta redundante, toda vez que estas ya se encuentran comprendidas en la categoría de "proveedores de servicios esenciales". Su mención expresa podría generar duplicidad de obligaciones y confusión interpretativa. Adicionalmente, el término "prestadores de servicios digitales" es demasiado amplio y carece de una definición precisa en el texto normativo, lo que genera incertidumbre jurídica sobre el alcance de las responsabilidades previstas. En la práctica, proveedores de nube, hosting o procesamiento de datos contemplan contractualmente mecanismos de notificación hacia sus clientes en caso de incidentes de seguridad. Imponerles la obligación de reportar directamente al ente rector implicaría duplicar responsabilidades y debilitar el principio de canal único de notificación. Por lo anterior, sugerimos ajustar la redacción de la disposición, de forma que se garantice mayor claridad y seguridad jurídica, evitando duplicidades. Una alternativa sería precisar el artículo en los siguientes términos: Texto propuesto: "*Artículo 20-J.- Responsabilidades del sector privado en materia de ciberseguridad.- Los proveedores de servicios esenciales y los operadores de infraestructura crítica digital deberán: (...)"* Respecto del literal c) consideramos importante precisar el alcance de la obligación de notificar incidentes relevantes al ente rector. Como se mencionó en el comentario anterior, los terceros que ofrecen soluciones tecnológicas — como proveedores de servicios en la nube, de alojamiento de contenido, procesamiento o disponibilidad— suelen incluir en sus contratos cláusulas específicas para notificar a sus clientes sobre cualquier incidente relevante.

		No obstante, estas notificaciones no se realizan de manera directa al ente rector, sino que corresponden al cliente afectado, en su calidad de responsable frente a la autoridad, trasladar dicha información si el incidente cumple con los criterios de relevancia establecidos. En ese sentido, sería conveniente aclarar en la redacción que la obligación recae sobre el cliente o entidad responsable ante el ente rector, y no directamente sobre los proveedores de soluciones tecnológicas, a fin de evitar duplicidad de reportes y cargas regulatorias que no se ajustan a las prácticas contractuales habituales del sector. En el literal d), establece lo siguiente: "d) Participar en simulacros, auditorías o ejercicios de ciberseguridad promovidos por el Estado." Al respecto, consideramos importante precisar que, si bien es adecuado que el Estado promueva simulacros y ejercicios de ciberseguridad como mecanismos de preparación y fortalecimiento de capacidades frente a incidentes, no resulta procedente incluir en la misma disposición las auditorías. Las auditorías corresponden a un proceso de naturaleza distinta, que implica mayor desarrollo técnico y normativo, así como reglas claras sobre alcance, metodologías, periodicidad y consecuencias derivadas de sus resultados. Su inclusión en este contexto puede generar ambigüedad y obligaciones desproporcionadas para los sujetos regulados. Por lo anterior, sugerimos respetuosamente excluir las auditorías del literal d. Finalmente, en relación con el último párrafo, que establece: "La normativa técnica establecer obligaciones diferenciadas según el nivel de riesgo y criticidad del servicio prestado", consideramos que la expresión "criticidad del servicio prestado" resulta ambigua, dado que no se encuentra definida ni se desarrollan los criterios para determinarla. Esto puede generar incertidumbre regulatoria al momento de clasificar las obligaciones. En caso de no precisarse el concepto ni establecer parámetros claros de medición, sería recomendable suprimir dicha referencia y limitar la disposición únicamente al nivel de riesgo, que cuenta con un entendimiento más estandarizado. • **Disposición Transitoria Tercera** Respecto de la disposición transitoria tercera, nuevamente el concepto de "prestadores de servicios digitales" resulta excesivamente amplio y no se encuentra definido en el proyecto de ley, lo que podría dar lugar a interpretaciones que excedan el ámbito material de la norma. En concordancia con lo ya señalado respecto al artículo 2, se recomienda que las obligaciones se circunscriban únicamente a las entidades públicas y a los operadores de infraestructura crítica digital. Adicionalmente, el plazo de noventa (90) días previsto para la implementación inicial resulta insuficiente frente a la complejidad técnica y operativa de las obligaciones de los artículos 20-C y 20-J. Para permitir una adecuación efectiva, se sugiere establecer un plazo mínimo de un (1) año a partir de la entrada en vigencia de la normativa técnica correspondiente. Texto Propuesto: "*TERCERA.- Las obligaciones previstas en los artículos 20-C y 20-J para operadores privados de infraestructura crítica digital y servicios esenciales*

		se aplicarán de manera progresiva según los niveles de criticidad y riesgo definidos por la normativa técnica que se expida. En todo caso, se garantizará un plazo mínimo de un (1) año, contado desde la entrada en vigencia de dicha normativa, para su implementación inicial." Mediante Oficio de fecha 27 de noviembre de 2025, la institución remitió nuevas observaciones al proyecto de ley, las cuales se encuentran disponibles en el siguiente enlace: https://drive.google.com/drive/folders/1z4gHk2GMo95fAvzHSb6MWzYX_TvuAzHA?usp=drive_link
9	**Centro Nacional De Inteligencia (CNI)**	• **Considerandos** Se observa que los artículos que sirven de base para la exposición de motivos del proyecto normativo, no mantienen el uso de la técnica legal o normativa al momento de su cita. • **Artículo 1** Literal g. Ciberseguridad; considerando que la ciberseguridad es un proceso de mejora continuo, se sugiere ampliar su definición a: Proceso basado en la aplicación de políticas, prácticas, controles y herramientas destinados a proteger todo sistema digital, electrónico, o de comunicaciones, así como las propiedades o dimensiones básicas de la información digital que almacenen o transmitan, siendo estas su confidencialidad, integridad y disponibilidad. Considerando la importancia del ciberespacio, el cual es considerado como el quinto dominio junto al mar, tierra, aire y espacio, se sugiere se discuta y añada su definición bajo el literal h en el artículo 5. • **Artículo 2** Se incorpore el siguiente texto: "Artículo 2.- Incorpórese los siguientes literales al artículo 7: p. Elaborar, mantener y actualizar de forma permanente un catálogo nacional de infraestructura crítica digital, en coordinación con las autoridades competentes." • **Artículo 20-C y 20-G** Establecen la obligación de notificar al ente rector en caso de incidentes relevantes, se sugiere se cambie la comunicación pertinente tanto al ente rector como a las partes pertinentes. Además, para garantizar una oportuna y apropiada comunicación de los hechos, se sugiere diseñar una estrategia de comunicación general, que sea aplicable a todas las organizaciones, instituciones y entidades sin importar su tamaño, definiendo roles y protocolos necesarios.
10	**Jorge Guerrón, Director de Proyectos**	• **Artículo 1** Se deben ampliar a los términos y definiciones incluyendo los de servicios esenciales e infraestructura crítica, para luego definir la infraestructura crítica digital. Establecer de manera clara cuáles son los diferentes elementos que van a conformar la infraestructura crítica y cómo el ministerio de

		telecomunicaciones siendo rector del sector estratégico de las telecomunicaciones va a ser el ente supervisor y regulador para otros sectores estratégicos como lo son por ejemplo la energía la salud y los que se definan en esta materia. Definir el mecanismo durante el cual se regularía otros sectores de seguridad digital para qué no se limite la capacidad del ministerio de telecomunicaciones de mantener su ámbito de competencia en el sector de las telecomunicaciones indicado en la CRE y que se pueda ampliar hacia los sectores de estratégicos. • **Artículo 2** El principal riesgo es el de que el MINTEL actúe como regulador, implementador y auditor, lo cual podría crear un conflicto de interés. Si el MINTEL es responsable de implementar políticas de seguridad de la información y, al mismo tiempo, es el ente encargado de supervisar y auditar dichas políticas, podría verse afectada su imparcialidad. En otras palabras, no sería un órgano completamente independiente al momento de evaluar el cumplimiento de las normas, lo cual ocurre actualmente. Esto va en contra de las buenas prácticas internacionales, que recomiendan la separación de funciones para evitar sesgos o manipulaciones. En modelos regulatorios más robustos y alineados con estándares internacionales, como los de la Unión Europea o incluso los de organismos como la ISO en cuanto a seguridad de la información (como la ISO 27001), la supervisión de la seguridad de la información suele ser realizada por entidades independientes, con mecanismos de control que no estén influenciados por el poder ejecutivo o legislativo. Este enfoque garantiza que las evaluaciones sean objetivas y se basen únicamente en criterios técnicos y de seguridad, sin interferencias políticas o de otro tipo como lo que ocurre en otros países. • **Artículo 20-D** El peligro normativo de que el MINTEL asuma tanto el rol de regulador como de supervisor en el ámbito de la seguridad de la información radica en la falta de imparcialidad y objetividad, lo cual podría generar confianza reducida tanto a nivel interno como internacional. La recomendación sería que se revisen los roles dentro del marco normativo y se busque garantizar la independencia en los procesos de auditoría y control. • **Sugerencias Adicionales** El MINTEL podría mantener su rol de desarrollo e implementación de infraestructura digital, pero sin la responsabilidad directa de la supervisión en cuanto a la seguridad de la información, lo que permitiría que expertos en ciberseguridad, de manera independiente, evalúen y fiscalicen las prácticas de seguridad en infraestructuras y redes. La experiencia de contar con órganos independientes resalta la importancia de la autonomía en la gestión de la seguridad de la información. El hecho de que estos órganos actúen como entes independientes de la regulación política y operen bajo marcos internacionales de ciberseguridad asegura una mejor transparencia, eficacia y objetividad en la aplicación de las normativas. En Ecuador, si el MINTEL o cualquier otro organismo estatal estuviera a cargo tanto de la creación como de la supervisión de políticas de seguridad de

		la información centralizando las actividades, no solo se corre el riesgo de conflictos de intereses, sino que también se puede poner en peligro la confianza internacional del país en términos de su cumplimiento con estándares internacionales de protección de datos y seguridad cibernética. Al concentrar tanto la implementación como la supervisión en una misma entidad (en este caso, el MINTEL), existe el riesgo de una centralización excesiva del poder en un solo organismo. Esto puede resultar en falta de transparencia, corrupción o inseguridad jurídica, ya que los actores del sector podrían sentir que las políticas son diseñadas en función de los intereses del gobierno o del MINTEL, más que por una verdadera necesidad de proteger la información y las infraestructuras críticas. Se debe segregar de manera clara y articulada que la gestión de la infraestructura tecnológica IT con la operación de la tecnología OT son dos áreas independientes pero relacionadas entre sí, desde el punto de vista de la protección, se deben involucrar diferentes normativas es decir, por un lado se puede considerar la ISA 62443º NERC (Sector Eléctrico y petróleo) para la gestión de operación de la tecnología y la ISO/IEC 27000 o NIST para la gestión de seguridad de la información en infraestructura de tecnología La actual propuesta normativa no fortalecería el ámbito de la ciberseguridad o seguridad digital del país al contrario seguiría manteniéndonos y estableciendo un marco en el cual no se eleve de manera adecuada las capacidades de protección de la infraestructura del Ecuador y menos aún de la infraestructura crítica ya que mantener el criterio actual desde la perspectiva de la seguridad de información estaría limitando las capacidades de los operadores de infraestructura crítica de gestionar los eventos y de relacionarse e interactuar de manera adecuada así como estaría entregando demasiadas atribuciones a un ministerio en el cual su contribución dentro de los sectores estratégicos ya se encuentra definido.
11	**Superintendencia de Bancos**	Los representantes de la Superintendencia de Bancos comparecieron ante la Comisión General en la Sesión Ordinaria N.º 25, de fecha 4 de septiembre de 2025, presentando los aspectos observados sobre el proyecto de ley. En relación con las observaciones remitidas por escrito mediante el Oficio Nro. SB-IG-2025-0118-O, de fecha 27 de agosto de 2025, se deja constancia de que su contenido guarda correspondencia relevante con lo expuesto en Comisión General; por tal razón, y a fin de mantener la sistematicidad del informe, se incorpora la documentación remitida de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1YWNUtoa06qdNnv7ZtI_eYFZi0LnlXUzt?usp=drive_link
12	**Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)**	Los representantes de ARCOTEL comparecieron ante la Comisión General en la Sesión Ordinaria N.º 24, de fecha 3 de septiembre de 2025, presentando los aspectos observados sobre el proyecto de ley. En relación con las observaciones remitidas por escrito mediante el Oficio Nro. ARCOTEL-ARCOTEL-2025-0290-OF, de fecha 28 de agosto de 2025, se deja constancia de que su contenido guarda correspondencia relevante con lo expuesto en Comisión General; por tal razón, y a fin de mantener la sistematicidad del informe, se incorpora la documentación remitida de manera íntegra para su consulta en el siguiente enlace:

		https://drive.google.com/drive/folders/1ncVLNDwjwRRACX8Awl8w1_wM8MISwgZB?usp=drive_link
13	**Superintendencia de Ordenamiento Territorial, Uso y Gestión Del Suelo (SOT)**	Los representantes de la SOT comparecieron ante la Comisión General en la Sesión Ordinaria N.º 29, de fecha 16 de septiembre de 2025, presentando los aspectos observados sobre el proyecto de ley. En relación con las observaciones remitidas por escrito mediante el Oficio Nro. SOT-DS-2025-0374-O, de fecha 29 de agosto de 2025, se deja constancia de que su contenido guarda correspondencia relevante con lo expuesto en Comisión General; por tal razón, y a fin de mantener la sistematicidad del informe, se incorpora la documentación remitida de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/126A5NgvDwG7fOaO9AAjoC4vx7Sfz3JMF?usp=drive_link
14	**Procuraduría General del Estado (PGE)**	• **Artículo 1** Analizar que el proyecto de Ley se denomina “Ley Orgánica para el Fortalecimiento de la Ciberseguridad Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual”, y en este mismo texto se incluye una reforma a la Ley Orgánica de Telecomunicaciones. • **Artículo 2** Previo a generar estos documentos o determinar la política de estado, se sugiere tomar en cuenta la Estrategia Nacional de Ciberseguridad del Ecuador, elaborada por el Ministerio de telecomunicaciones, en la que se estableció en el periodo de 2022 a 2025 como lo informa el Boletín Oficial N°61. • **Artículo 20-A** Se sugiere que la redacción contemple un enfoque también orientado a la prevención y anticipación de la amenaza. También especificar las responsabilidades y obligaciones tanto de las personas naturales como de las jurídicas en el cumplimiento de la ciberseguridad, esto ayudará a que todas las partes comprendan su rol y el nivel de protección requerido. Se sugiere considerar los principios detallados en la Estrategia Nacional de Ciberseguridad del Ecuador, emitido por Ministerio de telecomunicaciones. En el mismo sentido, se sugiere incluir un compromiso para fomentar la cultura de ciberseguridad a través de la educación ciudadana y la sensibilización en el uso seguro de tecnologías. Además, se recomienda incorporar una disposición que establezca programas de capacitación en ciberseguridad para el público en general, con talleres, cursos en línea y materiales educativos, con el fin de fomentar un uso seguro y consciente del ciberespacio. Del mismo modo, se sugiere considerar el Art. 4 de Ley de Seguridad Publica y del Estado, en relación a los principios ya desarrollados como por ejemplo, los de integridad, complementariedad, prioridad y oportunidad, y la responsabilidad.

		• **Artículo 20-B** Fomentar la adopción de tecnologías de seguridad avanzadas en las telecomunicaciones, como inteligencia artificial para la detección de amenazas y tecnologías de autenticación segura. • **Artículo 20-C** Dentro de las responsabilidades, se sugiere asegurar que los análisis de Big Data respeten los principios de anonimización y privacidad de datos personales, conforme la Ley de Protección de Datos Personales. Por ejemplo, incorporar una cláusula que exija la anonimización de datos personales antes de su análisis en procesos de Big Data, garantizando que la identidad de los ciudadanos no se exponga sin autorización. • **Artículo 20-D** Se sugiere considerar la Estrategia Nacional de Ciberseguridad del Ecuador, elaborada por el Ministerio de Telecomunicaciones, vigente para el período 2022-2025, según consta en el Boletín Oficial N° 61. El ente rector y las instituciones que la conforman podrían determinarse en la presente ley. • **Artículo 20-F** Considerar los principios detallados en la Estrategia Nacional de Ciberseguridad del Ecuador, emitido por Ministerio de telecomunicaciones. Otro principio sugerido es la Participación Ciudadana en la Cultura de Ciberseguridad: Incluir un compromiso para fomentar la cultura de ciberseguridad a través de la educación ciudadana y la sensibilización en el uso seguro de tecnologías. • **Artículo 20-J** Sobre la ejecución esta responsabilidad, de igual forma se sugiere promover y asegurar que los análisis de Big Data respeten los principios de anonimización y privacidad de datos personales, conforme la Ley de Protección de Datos Personales. Es necesario fortalecer o formalizar en los esquemas de talento humano de las instituciones del sector público la figura del Oficial de Seguridad de la Información. • **Artículo 4.- Ley Orgánica de Telecomunicaciones** Considerar nuevamente que, el Proyecto de Ley se denomina Ley Orgánica para el Fortalecimiento de la Ciberseguridad Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual, y en este mismo texto se incluye una reforma a la Ley Orgánica de Telecomunicaciones.
15	**Ministerio de Defensa Nacional**	• **Artículo 1** A continuación del literal g, se deberían incluir los términos que se indican. La incorporación de estos términos se justifica porque actualmente el proyecto de ley no delimita con precisión conceptos clave del ecosistema digital, lo que puede generar ambigüedad en su aplicación. Definir expresamente ciberdelitos, ciberdiplomacia, ciberinteligencia, CSIRT, auditoría de seguridad de la información y ciberataque permite alinear la

		normativa ecuatoriana con estándares internacionales (Convenio de Budapest, ISO/IEC 27000, NIST, OEA), dotar de mayor claridad jurídica a las instituciones responsables y garantizar un marco integral que abarque dimensiones técnicas, legales, operativas y estratégicas de la ciberseguridad. Esto fortalece la capacidad del Estado para prevenir, responder y cooperar en el ámbito nacional e internacional frente a amenazas en el ciberespacio. Se sugiere: h. Ciberdefensa. - Capacidad militar y tecnológica que poseen las Fuerzas Armadas, para ejecutar operaciones en y a través del ciberespacio, que permitan defender y responder a los ciberataques a la infraestructura crítica digital e información estratégica del Estado, así como apoyar el cumplimiento de operaciones para la defensa de la soberanía y la integridad territorial. (Estrategia de Ciberseguridad, 2022-2025). i. Ciberdelitos. Conductas ilícitas cometidas a través del uso indebido de sistemas, redes o servicios digitales, tipificadas en el Código Orgánico Integral Penal y en los instrumentos internacionales ratificados por el Ecuador. j. Ciberinteligencia. Capacidad institucional de recolectar, procesar y analizar información proveniente del ciberespacio, con el fin de anticipar amenazas, prevenir incidentes, apoyar la toma de decisiones estratégicas y proteger los intereses del Estado. k. CSIRT (Computer Security Incident Response Team). Equipo especializado encargado de gestionar incidentes de seguridad informática, mediante actividades de prevención, detección, análisis, respuesta y recuperación frente a ciberataques o vulneraciones digitales. l. Auditoría de seguridad de la información. Proceso sistemático, independiente y documentado para evaluar el cumplimiento de políticas, normas, controles y buenas prácticas en materia de seguridad de la información, con el fin de identificar vulnerabilidades y proponer medidas correctivas. m. Ciberataque. Acción maliciosa ejecutada a través del ciberespacio para alterar, interrumpir, dañar, acceder indebidamente o destruir sistemas, redes, servicios o información digital, que pueda afectar la seguridad, estabilidad y continuidad de las operaciones del Estado, empresas o personas. • **Artículo 20-A** Incluir en los principios de ciberseguridad uno adicional: Reconocimiento del ciberespacio como dominio estratégico. La Constitución ecuatoriana menciona telecomunicaciones y espectro radioeléctrico, pero no reconoce explícitamente el ciberespacio como dominio estratégico. Sin embargo, el acceso a internet como servicio de telecomunicaciones abre la puerta para definir al ciberespacio como un ámbito fundamental de soberanía y seguridad nacional, equiparable a los otros dominios.

		Con esto, el proyecto de ley no se sale del marco constitucional vigente y es pertinente para fundamentar el reconocimiento del ciberespacio como quinto dominio estratégico. Texto sugerido: *"h) Reconocimiento del ciberespacio como dominio estratégico. El ciberespacio es un entorno esencial para la seguridad, soberanía y desarrollo nacional, por lo que su protección constituye una responsabilidad compartida entre el Estado, el sector privado y la sociedad."* • **Artículo 20-G** A continuación del 3er. Párrafo del artículo 20-G, se debería incluir: que la notificación también deberá hacerse simultáneamente al ente responsable de la defensa de las infraestructuras críticas digitales (Comando de Ciberdefensa) Texto sugerido: "Artículo 20-G.- Obligación de notificación de incidentes de seguridad digital. • Suponga una vulneración de la seguridad que pueda escalar o propagarse. Paralelamente y de la misma manera, los operadores de la infraestructura crítica digital deberán notificar al ente responsable de la defensa de cualquiera de los incidentes antes mencionados." • **Artículo 20-H** Se debe especificar el ente rector del organismo al que se refiere. • **Artículo 20-I** Se debe especificar el ente rector del organismo al que se refiere. Además, el término "fiscalización" suele estar vinculado a ámbitos tributarios, administrativos o de control financiero, lo que puede generar ambigüedad en la aplicación de la norma. En el contexto de la ciberseguridad, el enfoque debe ser más técnico y especializado, por lo que resulta más preciso utilizar la expresión "auditorías de seguridad de la información", que refleja prácticas estandarizadas a nivel internacional (ISO 27001, NIST, ENS, etc.). Este cambio permite garantizar que las acciones del ente rector no se limiten a un control formal, sino que abarquen la evaluación técnica, detección de vulnerabilidades y verificación de cumplimiento en materia de seguridad digital, asegurando mayor claridad, pertinencia y efectividad en la norma. Texto sugerido: "Artículo 20-I.- Auditorías y medidas correctivas.- El ente rector en transformación digital podrá realizar auditorías de seguridad de la información a las entidades sujetas a esta ley, con el fin de verificar el cumplimiento de las obligaciones en materia de seguridad digital, identificar vulnerabilidades y disponer las medidas correctivas correspondientes."

		• **Artículo 20-K** Se debe evitar la ambigüedad especificando los organismos con los que se realizará las coordinaciones. Texto sugerido: "Artículo 20-K.- Cooperación internacional en ciberseguridad.- El ente rector, en coordinación con la Cancillería, con las autoridades rectoras en defensa, seguridad, protección de datos personales y otras entidades competentes, promoverá la cooperación internacional en ciberseguridad mediante: (…)" • **Artículo 4 de la Ley Orgánica de Telecomunicaciones** La Ley Orgánica de Telecomunicaciones vigente, en el Art. 24 solo contempla 28 numerales, por lo que, el numeral propuesto debería ser el 29. En el artículo 24, incorpórese como numeral 30 un texto adicional. Se debe incrementar un articulado que prohíba la prestación de servicios de telecomunicaciones en las áreas de seguridad como: CPL y CRS Texto sugerido: "30. Restringir la prestación de servicios de telecomunicaciones en las zonas de seguridad que sean establecidas por los respectivos mecanismos legales." • **Artículo 5.-** Renumérese el actual numeral 30 como numeral 31. Revisar el art. 5 por ambigüedad.
16	**Superintendencia De Protección de Datos Personales**	Los representantes de la Superintendencia de Protección de Datos Personales comparecieron ante la Comisión General en la Sesión Ordinaria N.º 25, de fecha 4 de septiembre de 2025, presentando los aspectos observados sobre el proyecto de ley. En relación con las observaciones remitidas por escrito mediante el Oficio Nro. SPDP-SPD-2025-0467-O, de 2 de septiembre de 2025, se deja constancia de que su contenido guarda correspondencia relevante con lo expuesto en Comisión General; por tal razón, y a fin de mantener la sistematicidad del informe, se incorpora la documentación remitida de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1XolZTYXooZeuPVWaNFos6KuncDbuHegc?usp=drive_link
17	**Econ. Juan Carlos Urgiles, Gerente General de la Cooperativa de Crédito Jardín Azuayo**	El señor Juan Carlos Urgiles compareció ante la Comisión General en la Sesión Ordinaria N.º 26, de fecha 8 de septiembre de 2025, presentando sus observaciones al proyecto de ley. En relación con las consideraciones remitidas posteriormente por correo electrónico, se deja constancia de que su contenido complementa lo expuesto en Comisión General; por tal razón, y a fin de mantener la sistematicidad del informe, se incorpora la documentación enviada de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1CPa_vBUMqZhBoOBeQjbWxmqzKrK94uPZ?usp=drive_link
18	**Asociación de Empresas de Telecomunicaciones (ASETEL)**	El señor Juan Carlos Urgiles compareció ante la Comisión General en la Sesión Ordinaria N.º 26, de fecha 8 de septiembre de 2025, presentando sus observaciones al proyecto de ley. En relación con las consideraciones remitidas posteriormente por correo electrónico, se deja constancia de que su

		contenido complementa lo expuesto durante su intervención en Comisión General. Por tal razón, y con el fin de mantener la sistematicidad y coherencia del informe, se incorpora la documentación enviada de manera íntegra, la cual se encuentra disponible para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1yiKNylrj8ZXyaRtkPQJQ-ZXUCJVkHrrC?usp=drive_link
19	**Consejo de la Judicatura**	• **Artículo 20-B y 20-G** Dispone que las entidades públicas implementen políticas de gestión de incidentes, y el artículo 20-G fija la obligación de notificación en un plazo máximo de 72 horas. No obstante, no se establecen niveles de criticidad, protocolos estandarizados de reporte ni lineamientos claros para la preservación de evidencias digitales. Este vacío puede afectar la trazabilidad y eficacia en la respuesta. • **Artículo 20-D** Otorga al ente rector amplias atribuciones de coordinación estratégica en ciberseguridad. Sin embargo, existe el riesgo de solapamiento con ARCOTEL y la Autoridad de Protección de Datos Personales. Se recomienda precisar las competencias para evitar duplicidad y garantizar eficiencia institucional. • **Artículo 20-E** Establece coordinación con la Autoridad de Protección de Datos Personales. No obstante, en la práctica pueden surgir incidentes que involucren simultáneamente brechas de datos y afectación de infraestructura crítica. En estos casos, sería recomendable la definición de protocolos específicos de coordinación interinstitucional para evitar contradicciones en las obligaciones de reporte y sanción. • **Artículo 20-H** Establece criterios de identificación y clasificación de infraestructura crítica. Sin embargo, no contempla la obligación de auditorías periódicas, pruebas de resiliencia ni ejercicios de simulación. Estos mecanismos deberían incluirse para fortalecer la prevención y preparación frente a incidentes. • **Artículo 20-I** Otorga al ente rector facultades de fiscalización y medidas vinculantes. Sin embargo, no se prevé un mecanismo de coordinación con otros órganos de control como la Contraloría o ARCOTEL, lo que puede derivar en duplicidad sancionatoria. • **Artículo 20-J** Exige la implementación de sistemas de gestión basados en estándares internacionales (ISO 27001, NIST). Aunque positivo, no se contemplan plazos diferenciados para su cumplimiento según la criticidad o madurez tecnológica de los prestadores de servicios, lo que puede generar cargas desproporcionadas para operadores de menor escala.

20	**Ministerio del Interior**	• **Artículo 1** Sugiere agregar luego del artículo 1, como literal "e" lo siguiente: "e. Reconocer expresamente las competencias del Ministerio del Interior, a través de la Policía Nacional, en la prevención, investigación y persecución de los delitos informáticos y conductas ilícitas en entornos digitales, garantizando la protección de los derechos en entornos digitales." La inclusión del literal e) se realiza con el propósito de subsanar la omisión existente en el proyecto, que prioriza la economía digital y la transformación digital, pero omite reconocer la dimensión de seguridad pública y persecución penal que necesariamente conlleva la ciberseguridad. Al incorporar un literal específico que reconozca las competencias del Ministerio del Interior y de la Policía Nacional, se asegura coherencia con: el artículo 227 de la Constitución, que dispone que la administración pública se rige por los principios de eficacia, eficiencia, calidad, jerarquía y coordinación; el artículo 393 de la Constitución, que establece que el Estado garantizará la seguridad integral de las personas a través de la Policía Nacional; y el artículo 61 numeral 11 del COESCOP, que asigna a la Policía Nacional la función de "prevenir e investigar la delincuencia común y organizada, nacional y transnacional". La propuesta permite evitar un vacío normativo que podría dificultar la articulación institucional en la lucha contra los ciberdelitos, fortaleciendo la eficacia administrativa y garantizando que la normativa no contraríe la Constitución ni el marco legal vigente. • **Artículo 20-B** Se sugiere agregar, como segundo párrafo, el siguiente texto: *"(...) El ente rector emitirá directrices técnicas para la aplicación de estas medidas y establecerá protocolos de coordinación institucional, en los cuales se reconocerá expresamente la competencia del Ministerio del Interior, a través de la Policía Nacional, en la prevención, investigación y persecución de los delitos informáticos que se generen o evidencien en el marco de dichos incidentes."* El texto actual regula la gestión de incidentes en el ámbito administrativo, pero no incluye la dimensión penal que corresponde a los ciberdelitos. Al no reconocer al Ministerio del Interior y a la Policía Nacional, se genera un vacío de competencia que puede afectar la eficacia en la respuesta estatal. La inclusión expresa de estas instituciones asegura la coordinación con las funciones de seguridad pública y se ajusta al art. 393 de la Constitución, que impone al Estado garantizar la seguridad integral de las personas, así como al art. 61 numeral 11 del COESCOP, que asigna a la Policía Nacional la función de "prevenir e investigar la delincuencia común y organizada, nacional y transnacional. • **Artículo 20-C** Se sugiere agregar, como segundo párrafo, el siguiente texto:

		"(...) En los casos en que los incidentes configuren delitos informáticos, se deberá notificar también al Ministerio del Interior, a través de la Policía Nacional, para su investigación y persecución conforme a la ley." El reporte exclusivo al ente rector (MINTEL) invisibiliza la competencia de las instituciones de seguridad pública. En la práctica, muchos incidentes constituyen delitos informáticos que requieren investigación penal. La propuesta asegura la articulación entre la notificación administrativa y la persecución penal, en línea con el principio de eficacia administrativa previsto en el artículo 227 de la Constitución, que obliga a la coordinación entre entidades públicas; así como con el artículo 61 numeral 11 del COESCOP, que asigna a la Policía Nacional la función de "prevenir e investigar la delincuencia común y organizada, nacional y transnacional". • **Artículo 20-D** Texto propuesto: *"Artículo 20-D.- Coordinación estratégica en ciberseguridad.- El ente rector en transformación digital liderará la formulación y evaluación de la política pública nacional en materia de ciberseguridad, en coordinación con las autoridades rectoras en defensa, con el Ministerio del Interior como ente rector en seguridad ciudadana a través de la Policía Nacional en materia de ciberdelincuencia, con la autoridad de protección de datos personales y con otras entidades competentes, limitado a lo que concierne al diseño de estrategias y marcos normativos relacionados con la prevención, gestión de riesgos, protección de infraestructura crítica y derechos afectados por incidentes cibernéticos."* La redacción actual menciona de manera genérica a las "autoridades rectoras en seguridad", lo que genera ambigüedad y puede dar lugar a interpretaciones restrictivas. Debe especificarse expresamente al Ministerio del Interior y a la Policía Nacional, por ser las instituciones responsables de la prevención, investigación y persecución de ciberdelitos. Esta inclusión garantiza coherencia con el artículo 393 de la Constitución, que establece que el Estado garantizará la seguridad integral de las personas a través de la Policía Nacional, y con el artículo 61 numeral 11 del COESCOP, que asigna a la Policía Nacional la función de "prevenir e investigar la delincuencia común y organizada, nacional y transnacional". De esta forma se asegura la correcta articulación institucional, se evita duplicidad o vacíos de competencia y se fortalece la capacidad del Estado para enfrentar los riesgos de la ciberdelincuencia en el marco de la política pública de ciberseguridad • **Artículo 20-F** Texto Propuesto: "*Artículo 20-F.– Coordinación operativa para la implementación de la política de ciberseguridad.- El ente rector en transformación digital coordinará con las entidades responsables de defensa, seguridad ciudadana incluyendo expresamente al Ministerio del Interior y a la Policía Nacional en materia de ciberdelincuencia, salud, justicia, educación, inclusión y protección de datos personales, 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. *Esta coordinación se realizará en conjunto con las entidades competentes, a través de convenios interinstitucionales, comités técnicos especializados o instrumentos de planificación, conforme a lo establecido en esta ley y su normativa técnica."* La referencia genérica a la "seguridad" en este artículo debe entenderse tanto en el ámbito de la seguridad nacional como en el de la seguridad ciudadana. En este último ámbito, el órgano competente es el Ministerio del Interior, como ente rector en seguridad ciudadana, y la Policía Nacional, en cumplimiento de sus atribuciones constitucionales y legales. Su inclusión expresa evita ambigüedad normativa y asegura una coordinación interinstitucional efectiva frente a incidentes que constituyan infracciones penales. Esta precisión es coherente con el artículo 393 de la Constitución, que dispone que el Estado garantizará la seguridad integral de las personas a través de la Policía Nacional, y con el artículo 61 numeral 11 del COESCOP, que asigna a la Policía Nacional la función de "prevenir e investigar la delincuencia común y organizada, nacional y transnacional". De esta manera, se fortalece la articulación institucional y se garantiza que la política operativa de ciberseguridad contemple de forma expresa la dimensión penal, junto con las acciones administrativas y técnicas de prevención y gestión de riesgos digitales. • **Artículo 20-G** Sustitúyase el último párrafo y agréguese: *"(...) La notificación deberá realizarse en un plazo máximo de setenta y dos (72) horas desde su detección, de conformidad con los protocolos que establezca el ente rector.* *En los casos que involucren información sensible para investigaciones judiciales o de inteligencia, los reportes deberán garantizar la reserva y confidencialidad de la información, estableciendo protocolos de coordinación con el Ministerio del Interior, la Policía Nacional y la Fiscalía General del Estado."* La obligación de notificar en un plazo máximo de setenta y dos (72) horas constituye un avance positivo en materia de gestión de incidentes de seguridad digital. Sin embargo, el texto original no prevé excepciones en los casos en que la información sea sensible para investigaciones judiciales o de inteligencia, lo que puede comprometer su eficacia y vulnerar garantías procesales. La propuesta incorpora una cláusula de reserva y coordinación interinstitucional con el Ministerio del Interior, la Policía Nacional y la Fiscalía General del Estado, a fin de asegurar un equilibrio entre la necesaria transparencia y el deber de proteger los derechos fundamentales. Esta inclusión se ajusta al artículo 66 numeral 19 de la Constitución (protección de datos personales) y al artículo 76 de la Constitución (debido proceso y derecho a la defensa).

		• **Artículo 20- I** Texto propuesto: "*Artículo 20-I.- Fiscalización y medidas correctivas.- El ente rector podrá realizar acciones de fiscalización técnica a las entidades sujetas a esta ley, a fin de verificar el cumplimiento de las obligaciones en materia de seguridad digital. En caso de incumplimiento, podrá disponer:* *a) Instrucciones técnicas vinculantes para subsanar deficiencias;* *b) Medidas de prevención o contención de riesgos; y,* *c) Requerimientos de capacitación o de auditoría externa.* *En caso de reincidencia o negativa a implementar las disposiciones emitidas, se informará a las autoridades competentes para la imposición de sanciones administrativas, conforme al régimen jurídico aplicable."* Cuando de dichas acciones se deriven posibles delitos informáticos, el ente rector deberá remitir inmediatamente la información correspondiente al Ministerio del Interior, a la Policía Nacional y a la Fiscalía General del Estado, para que actúen en el marco de sus competencias El artículo otorga al ente rector facultades de fiscalización en materia de seguridad digital, pero no establece un canal de comunicación con las autoridades penales en los casos en que se evidencien posibles delitos informáticos. Esta omisión puede provocar duplicidad institucional o ineficacia en la persecución penal. La propuesta asegura que los hallazgos que constituyan delitos sean inmediatamente remitidos al Ministerio del Interior, a la Policía Nacional y a la Fiscalía General del Estado, en concordancia con el principio de legalidad penal, que impone al Estado el deber de actuar ante toda infracción tipificada, y con el principio de cooperación interinstitucional derivado del artículo 227 de la Constitución. Asimismo, se refuerza la competencia del artículo 61 numeral 11 del COESCOP, que asigna a la Policía Nacional la función de "prevenir e investigar la delincuencia común y organizada, nacional y transnacional". De esta forma se garantiza una adecuada articulación entre el control administrativo y la persecución penal, fortaleciendo la eficacia del sistema de ciberseguridad estatal. • **Artículo 20-J** Agréguese al último párrafo lo siguiente: *"(...) Cuando los incidentes notificados constituyan indicios de delitos informáticos, estos deberán ser remitidos de manera inmediata al Ministerio del Interior, a través de la Policía Nacional, sin perjuicio de la notificación al ente rector."* El sector privado gestiona datos y servicios críticos cuya afectación puede generar consecuencias de carácter penal. Limitar la obligación de notificación únicamente al ente rector en transformación digital debilita la capacidad de respuesta del Estado frente a la ciberdelincuencia.

		• **Sugerencias Adicionales** En el artículo 3, de la Ley Orgánica para la Transformación *Digital y Audiovisual, efectúese la siguiente reforma:* *"Art.3.- Rectoría. El ente rector en materia de telecomunicaciones será la entidad rectora en transformación digital y gobierno digital, para lo cual ejercerá atribuciones y responsabilidades, así como emitirá las políticas, directrices, acuerdos, normativa y lineamientos necesarios para su implementación.* *En el ámbito específico de la prevención, investigación y persecución de los delitos informáticos y conductas ilícitas en entornos digitales, la rectoría sectorial corresponderá al Ministerio del Interior, a través de la Policía Nacional, de conformidad con sus atribuciones legales y constitucionales, manteniendo la necesaria coordinación interinstitucional con el ente rector en transformación digital."* La Dirección de Ciberdelitos advirtió que asignar la rectoría exclusiva al Ministerio de Telecomunicaciones invisibiliza a las instituciones responsables de la seguridad ciudadana y del orden público, generando un diseño institucional incompleto. Conforme al artículo 393 de la Constitución, el Estado debe garantizar la seguridad integral de las personas, y en ese marco la prevención e investigación de ciberdelitos corresponde al Ministerio del Interior y a la Policía Nacional. Asimismo, el artículo 63 del COESCOP establece que corresponde al Ministerio del Interior ejercer la rectoría sectorial sobre la Policía Nacional, lo cual refuerza su competencia en esta materia. En consecuencia, la propuesta de texto busca articular dos dimensiones complementarias: la transformación digital y el gobierno digital bajo la rectoría del MINTEL, y la ciberdelincuencia y seguridad digital bajo la competencia del Ministerio del Interior y la Policía Nacional. De esta manera se asegura coherencia normativa, se evitan vacíos de competencia y se fortalece la capacidad estatal frente a los delitos cometidos en entornos digitales, en concordancia con los principios de eficacia, coordinación y jerarquía previstos en el artículo 227 de la Constitución. -En el artículo 19, de la ley ibidem: "*Art 19.- Gestión del Marco de Seguridad Digital. El Marco de Seguridad Digital del Estado se tendrá que observar y cumplir con lo siguiente:* *"(...) d. Notificación de incidentes: Las entidades públicas y privadas deberán reportar incidentes de seguridad digital en un plazo máximo de setenta y dos (72) horas. Dicho reporte garantizará la reserva y confidencialidad de la información sensible relacionada con investigaciones judiciales o de inteligencia, conforme a protocolos definidos conjuntamente por el Ministerio del Interior, la Fiscalía General del Estado y las autoridades competentes."* La Dirección de Ciberdelitos observó que si bien el artículo distribuye competencias entre Defensa, Inteligencia y Justicia, no establece reglas claras para la confidencialidad y reserva de la información en los reportes de incidentes de seguridad digital. Esta omisión puede comprometer la

		integridad de procesos judiciales y de inteligencia, además de vulnerar derechos fundamentales de los titulares de la información. La propuesta de adicionar un literal sobre notificación de incidentes subsana dicha omisión, al equilibrar la obligación de transparencia y reporte de incidentes con la necesidad de proteger procesos judiciales y de inteligencia. Con ello se asegura coherencia con el artículo 66 numeral 19 de la Constitución (protección de datos personales), el artículo 76 (debido proceso), el artículo 393 de la Constitución (seguridad integral garantizada por la Policía Nacional), así como con el artículo 61 numeral 11 del COESCOP (función de la Policía Nacional de prevenir e investigar la delincuencia común y organizada, nacional y transnacional). Adicionalmente, se mantiene concordancia con la LOTAIP, que prevé la reserva de información en casos de seguridad nacional o investigaciones en curso.
21	**Abg. Juan Pablo González**	• **Artículo 20-B** Nada indica el Proyecto de Ley sobre el enfoque de gestión y evaluación de riesgo cibernético y por ende, la necesidad de adoptar medidas para mitigarlos, como además la necesidad de establecer un sistema de gestión de seguridad, planes de continuidad operativa y recuperación ante incidentes por parte de los sujetos obligados. Tampoco, se señala la obligación de realizar auditorías internas y externas de carácter periódicas. A mayor detalle, el artículo 20-B "Gestión de incidentes digitales" se centra en el sector público en cuanto deber de implementar políticas y procedimientos para la gestión de incidentes digitales; solo vinculándose con el artículo 20-J a propósito de la responsabilidad del sector privado, únicamente aplicable a "prestadores de servicios digitales, entidades financieras, proveedores de servicios esenciales y operadores de infraestructura crítica", que no son definidos a lo largo de la reforma propuesta, y que, por lo tanto, también es importante tener en consideración otros actores de los cuales exista dependencia a nivel crítico de ciberseguridad en el país. • **Artículo 20-G** En cuanto a la obligación de incidentes, se establece un plazo de 72 horas y establece sanciones por temas de omisión, pero no sé indica en el artículo 20-G a cuál corresponde. Esta obligación sólo es aplicable a entidades públicas, prestadores de servicios digitales y operadores de infraestructura crítica digital, y los criterios por los cuales debe reportarse un incidente serían: (a) comprometa la disponibilidad, confidencialidad o integridad de datos personales o institucionales; (b) afecte la continuidad operativa de servicios esenciales o críticos; (c) suponga una vulneración de la seguridad que pueda escalar o propagarse. No se profundiza en otros criterios, ni se definen términos tales como: "servicio esencial o crítico". En el caso de Chile, el reporte de incidentes se establecen reportes diferenciados (3 horas alerta temprana; 24 horas para informe intermedio y en el caso de operadores de importancia vital, 72 horas; y 15 días para el Informe final), debiendo solo realizarse en aquellos casos en que el incidente reúna los requisitos para ser considerado de impacto significativo.

		Nada se indica sobre la creación de un Registro de incidentes cibernéticos que les permita compartir información con otros CSIRT sectoriales o regionales, lo que le permitiría facilitar el análisis de tendencias y respuesta coordinada. Tampoco se establece un esquema escalonado según severidad e impacto, como lo establecen las normativas en la región. Es importante que esta obligación aborde de manera coordinada a todos los entes dentro del Estado Ecuatoriano que puedan tener una implicancia en la ciberseguridad, debido a la importancia para mejorar la respuesta y coordinación ante incidentes informáticos. • **Artículo 20-H** El Proyecto de Ley, otorga competencia al Ministerio de Telecomunicaciones, debiendo este establecer el listado de catálogo nacional de infraestructura crítica digital; clasificación que será en base a la protección según impacto, interdependencia y sensibilidad en coordinación con las entidades responsables de sectores estratégicos. Es importante mencionar estos servicios serán únicamente para aquella infraestructura y servicios digitales, dejando de lado otros posibles sectores críticos, que no están definidos ni se indican en la reforma propuesta. En el caso de Chile, la ANCI tiene el rol de clasificar de aquellos sectores esenciales, en que se incluyen diversos sectores económicos, aquellos que serán operadores de importancia vital; mientras que, en el caso de el Salvador, la ACE tiene la labor de proteger ciertos sectores, tales como: telecomunicaciones, energía y finanzas. Una de las dificultades que se presentan en el Proyecto es que se centra en los proveedores de servicios de tecnología y digitales, y no se extiende a otros sectores económicos relevantes para el país; además, la formulación de los mismos queda limitado a un Ministerio, no estableciéndose un sistema de evaluación periódica de riesgos, que es necesario para la clasificación o catálogo de “Infraestructuras Críticas”, que permite determinar su criticidad no solo a nivel de sector u operador, sino a nivel de sistema(s) informático(s), para que todos los actores interesados puedan enfocar estratégicamente sus esfuerzos en la protección de aquello que es realmente “crítico”. • **Artículo 20-I** El Proyecto no establece de manera clara la tipificación y sanciones frente al incumplimiento de las obligaciones señaladas, indicando únicamente que el Ministerio de Telecomunicaciones deberá realizar fiscalización técnica de las entidades sujetas a la normativa, y que en caso de reincidencia o negativa, se informará a las autoridades competencias para las sanciones administrativas, realizando una remisión a otras disposiciones pero sin indicarse de manera expresa; tampoco se señala cuáles son estas competencias que tienen estos reguladores. A su vez, a diferencia de la Directiva NIS2, nada se indica sobre las posibles responsabilidades para la Alta Dirección, y, por ende, especialmente en el sector privado en que debe tener un rol preponderante en la supervisión directa de política en estas materias. El sector privado solo tiene responsabilidades que serán fijadas posteriormente por la normativa técnica que dicte el Ministerio de Telecomunicaciones, acorde al artículo 20-J.

		Además, nada se indica sobre umbrales de las multas, por ejemplo la Directiva NIS2 establece sanciones de hasta 10 millones de euros o el 2% de la facturación anual global por incumplimiento; que debiese tener en consideración aspectos de proporcionalidad, como el tamaño y criticidad de la entidad; en el caso de la normativa Chilena, se establece multas hasta 20.000 UTM para los servicios esenciales y hasta 40.000 UTM en el caso de operadores de importancia vital, lo que puede ser un desincentivo para el cumplimiento de las obligaciones indicadas en la reforma que se propone. • **Artículo 20-K** Se propone la creación de un Comité Nacional de Ciberseguridad establecido como una instancia interinstitucional que es presidido por el Ministerio y dicta resoluciones que son vinculantes para el sector público (art. 20-L). Si uno analiza otras legislaciones en la región, particularmente la Ley N 21.663 de Chile, se crea una Agencia especializada (ANCI), y en el caso del Decreto No. 143 de El Salvador, se crea la Agencia de Ciberseguridad del Estado (ACE). Puede que por limitaciones de índole constitucional o legal, impida la creación de una autoridad y se otorga la competencia al Comité, presidido por el Ministerio de Telecomunicaciones. Sin embargo, una de las dificultades que se puede generar, es que el Comité Nacional de Ciberseguridad, será un ente asesor del Ministerio, no cuente con presupuesto y por ende, no sea una instancia permanente, ni cuente con atribuciones claras que le permitan fiscalizar, emitir directrices y, por lo tanto, tener una activa coordinación con otras entidades ministeriales para actividades tales como: simulacros nacionales, propios de una autoridad especializada en la materia. Tampoco se señala de manera clara la coordinación que tiene con otras entidades de gobierno, quedando relegado todo a disposición reglamentaria. Sin perjuicio de ello, se indica que las resoluciones que dicte el Comité, tendrán el carácter de vinculantes para el sector público, sin entrar en detalle si ello puede conllevar sumarios administrativos u otras acciones a nivel administrativo. • **Disposición Transitoria Primera** El Proyecto de Ley establece un plazo de 180 días en que el Ministerio de Telecomunicaciones debe dictar una normativa técnica, y 90 días para una aplicación progresiva para el sector privado en aquellos operadores privados. Sin perjuicio de ello, la modificación a la Ley entra en vigor una vez publicada en el Diario Oficial. En el caso de la normativa Chile, su entrada en vigor fue establecida en plazos, lo que se concretó durante enero y marzo del 2025, sin perjuicio que en el caso de los operadores de importancia vital recién serán declarados a finales de año de 2025. En el caso de la normativa de El Salvador, si bien no sé indica específica, se señala que habrá una implementación de carácter gradual • **Sugerencias Adicionales** En el Proyecto de Ley no se hace mención sobre la creación de un Equipo ante Respuesta a Incidentes Cibernéticos (CSIRT) a nivel nacional, mientras que en otras normativas de la región (ej. Chile) e inclusive a nivel reglamentario, si se crea dicho organismo.

		Por otro lado, solo se menciona en el Proyecto, de alto nivel, la necesidad de fortalecer el rol de Ecuador en esta materia y, por ende, formalizar la adhesión a redes como FIRST; CSIRT Américas y Convenio de Budapest, además, de establecer acuerdos bilaterales de asistencia mutua, pero sin indicarse expresamente la necesidad de crearse un equipo especializado. Nada se indica sobre el rol del Ministerio de Relaciones Internacionales y Exteriores sobre su eventual rol como punto focal nacional para coordinación ante respuesta de incidentes de carácter transfronterizo.
22	**Cámara de Innovación y Tecnología Ecuatoriana (CITEC)**	Los representantes de CITEC comparecieron ante la Comisión General en la Sesión Ordinaria N.º 33, de fecha 29 de septiembre de 2025, presentando sus observaciones al proyecto de ley. En relación con los criterios remitidos posteriormente mediante el Oficio N.º OFICIO-CITEC-059-2025, de 18 de septiembre de 2025, se deja constancia de que su contenido complementa lo expuesto en Comisión General; por tal razón, y a fin de mantener la sistematicidad del informe, se incorpora la documentación enviada de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1No6GP6Pu-YILjnSo_6-PINp0Ez-O2SiL?usp=drive_link
23	**Contraloría General del Estado (CGE)**	• **Exposición de Motivos** Desde las instituciones públicas la implementación de una estrategia de ciberseguridad, seguridad de la información y protección de datos personales requiere de un equipo altamente capacitado en aspectos técnicos. Actualmente para la implementación del EGSI se requiere una persona que no sea de TICs para evitar el conflicto de intereses, sin embargo, la falta de conocimiento complica la implementación. Para evitar esta limitante se recomienda que se disponga la creación de la figura de Oficial de Seguridad al interior de las instituciones, con recursos a un nivel de asesor o director debido a que en ocasiones se deberá convertir en una Dirección o Gerencia de Seguridad de la Información y Ciberseguridad. El ministerio de finanzas deberá garantizar los recursos para el cumplimiento normativo y el Ministerio de Trabajo deberá definir el perfil técnico para el desarrollo de las actividades. • **Artículo 2** Conforme a lo determinado en el literal p), se recomienda hacer un catastro nacional de entidades públicas mismo que permita una categorización de entidades públicas acorde a la sensibilidad de la información que manejan, el presupuesto asignado y la capacidad operativa, esto permitirá focalizar los esfuerzos de control. Además, la infraestructura crítica deberá ser reportada de manera obligatoria a la Contraloría General del Estado a través de los medios que este defina. A su vez la CGE definirá los medios de consulta para el ente rector en materia de telecomunicaciones por ser la entidad rectora en transformación digital y gobierno digital. Conforme a lo relacionado al literal q. El artículo 211 de la CRE y en concordancia con el artículo 23.3 referente a la auditoría informática de la Ley Orgánica de la Contraloría General del Estado. Conforme al análisis esto evita

		duplicidad de funciones entre los órganos rectores conforme al ámbito de sus competencias. En cuanto al literal r. Se recomienda definir una estrategia Nacional de Ciberseguridad para apoyar a las entidades que no cuentan con capacidad operativa para hacer frente a estas circunstancias, además el equipo de las instituciones que sean categorizadas dentro del nivel que puede contar con equipo debería ser convocado para apoyar a las entidades pequeñas. En relación al literal u. Se recomienda generar un repositorio de estándares para la adopción por parte de las entidades del sector público. • **Artículo 20-B** Alinear esfuerzos desde una Estrategia Nacional para evitar que existan instituciones que no puedan hacer frente a las amenazas. • **Artículo 20-C** El "adoptar medidas para garantizar" deja un esquema ambiguo, la justificación debe definir exactamente las certificaciones en el cumplimiento de estándares de seguridad verificables por entidades certificadores conforme a estándares internacionales. • **Artículo 20-G** La ponderación deber ser conforme una gestión de riesgos, basada en la ponderación del Catastro Nacional de Entidades Públicas administrado por la CGE, únicamente las entidades con capacidad operativa hacen el reporte. Las que no cuenten con capacidad deberán solicitar apoyo a las entidades que cuenten con estructuras de seguridad • **Artículo 20-H** El reporte se debería realizar Catastro Nacional de Entidades Públicas administrado por la CGE para realizar la ponderación de riesgos y alinear al Plan Nacional de Control • **Artículo 20-I** Esto es un examen especial de la CGE.
24	**Unidad de Análisis Financiero y Económico (UAFE)**	• **Artículo 20-G** Se sugiere incluir un inciso final que disponga lo siguiente: “En el caso de que el ente rector en transformación digital, conozca de información relevante que puede constituir un delito de lavado de activos o financiamiento de otros delitos, deberá ponerlo en conocimiento de la Unidad de Análisis Financiero y Económico, así como de la Fiscalía General del Estado, a fin de combatir los incidentes cibernéticos representen una amenaza o lesionen un bien jurídico.” • **Artículo 20-H** Se sugiere incluir el siguiente numeral: “d. Los indicadores de riesgo potencial.”

		• **Artículo 20-K** Se sugiere incluir el siguiente numeral: "c. Intercambio informal de información sobre incidentes cibernéticos."
25	**Andrea Paulina Tenesaca Quizhpe, Master en Ciberseguridad y Especialista en Seguridad de la Información**	Durante las Sesiones N.º 39, 41, 43 y 44, realizadas los días 23, 28 29 y 30 de octubre de 2025, diversos comparecientes expusieron ante la Comisión General sus observaciones y criterios respecto del proyecto de ley. En relación con la documentación adicional remitida posteriormente por correo electrónico, se deja constancia de que su contenido complementa y desarrolla lo manifestado durante dichas comparecencias; por tal razón, y a fin de mantener la sistematicidad y coherencia del informe, se incorpora la documentación enviada de manera íntegra para su consulta en el siguiente enlace: https://drive.google.com/drive/folders/1r8t6eq1BNnrBNAl2ekW2Fcmo888ytWLG?usp=sharing
26	**Ola Bini, Director Técnico – Seguridad Digital EC**	
27	**Sr. Omar Durazno, Experto en Seguridad**	
28	**Gabriel Brito Collantes, Antropólogo Digital**	
29	**Sr. Patricio Quevedo, Apoderado especial y Procurador Judicial de la Compañía Starlink**	
30	**Sr. Julio Rosas, Experto en Ciberseguridad**	
31	**Sr. Alejandro Mero, Experto en Ciberseguridad**	
32	**Sr. Mario Cubero, Experto en Ciberseguridad**	
33	**Sara Zambrano Vizcaíno Directora Ejecutiva, Centro de Autonomía Digital**	El proyecto reconoce a la ciberseguridad como un componente clave, estructural y habilitante para una transformación digital legítima, segura y sostenible del Estado ecuatoriano. Busca proteger la infraestructura crítica digital bajo principios técnicos de proporcionalidad, gestión de riesgos, continuidad operativa y coordinación entre sector público, privado, academia y sociedad civil. Se armoniza con la Ley Orgánica de Protección de Datos Personales (LOPDP), respetando su autonomía. **Potenciales riesgos para los derechos humanos** 1. Privacidad y vigilancia excesiva: La coordinación con organismos de defensa e inteligencia, junto con la fiscalización técnica y la gestión de incidentes, pueden abrir paso a prácticas de vigilancia masiva o indebida sin controles independientes efectivos, poniendo en riesgo la privacidad y la confidencialidad de datos. 2. Libertad de expresión y protesta: La criminalización de conductas digitales bajo la excusa de proteger infraestructura crítica puede

		limitar derechos fundamentales como la libertad de expresión y la protesta social digital. 3. Exclusión digital y acceso a la información: La digitalización acelerada puede profundizar desigualdades si no se garantiza acceso universal, alfabetización digital y políticas inclusivas para no dejar rezagados a grupos vulnerables. 4. Soberanía digital y dependencia tecnológica: Continuar confiando en grandes empresas tecnológicas internacionales (Big Tech) para infraestructura y servicios vulnera la soberanía digital del país, exponiendo al Estado a riesgos de pérdida de control sobre datos sensibles y procesos críticos. 5. Cifrado y seguridad tecnológica: Presiones para la introducción de backdoors o accesos especiales en tecnologías de cifrado comprometen la seguridad e integridad de las comunicaciones, aumentando riesgos para la privacidad y la protección frente a ataques. **Consideraciones sobre convenios internacionales** La adhesión al Convenio de Budapest y la Convención de la ONU contra el Cibercrimen tienen implicaciones en: - La posible criminalización excesiva de acciones digitales legítimas que afectan libertades digitales. - Acceso amplio y potencialmente problemático a evidencias electrónicas, afectando garantías judiciales y privacidad. - Dificultades para mantener la confidencialidad y seguridad tecnológica si se ceden controles a niveles internacionales sin protección nacional fuerte. **Recomendaciones clave:** - Incorporar salvaguardas claras para proteger la privacidad y limitar el acceso de organismos oficiales, garantizando supervisión independiente y rendición de cuentas. - Defender el cifrado fuerte y rechazar medidas que debiliten la seguridad tecnológica. - Fomentar una transformación digital incluyente, con énfasis en acceso universal, alfabetización digital y reducción de brechas. - Fortalecer capacidades técnicas internas para construir soberanía digital mediante inversión en talento local, desarrollo tecnológico propio e infraestructuras autónomas. - Garantizar la participación de la sociedad civil y transparencia en la formulación, implementación y evaluación de políticas públicas. - Evitar la duplicidad funcional y respetar plenamente la autonomía de la autoridad de protección de datos personales.

2.5. Detalle de la socialización realizada por la Comisión Especializada Permanente y Ocasional.

La Comisión de Soberanía, Integración y Seguridad Integral, durante un total de 15 sesiones, socializó, analizó y debatió el presente proyecto de Ley, para cuyo efecto se realizó las siguientes convocatorias:

Sesión / Fecha	Puntos Tratado
Sesión Nro. 20 18 de agosto de 2025	PUNTO ÚNICO: En el marco del tratamiento del Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual, recibir en comisión general a: 1. Asambleísta por Tungurahua Lenin Alejandro Lara Pérez 2. Diego Urbina Fletcher Delegado de Amazon Web Services 3. Ab. Juan Francisco Cabezas Martínez
Sesión Nro. 24 03 de septiembre de 2025	PUNTO ÚNICO: En el marco del tratamiento del Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual, recibir las observaciones de: 1. Mgtr. Marco Gallardo Ávila – Gerente Nacional de Ciberseguridad y Control de CNT. 2. Ing. Livington Briones – Coordinador Técnico de Control de la ARCOTEL
Sesión Nro. 25 04 de septiembre de 2025	PUNTO ÚNICO: En el marco del tratamiento del Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual, recibir las observaciones de: 1. Eco. Roberto Romero Von Buchwald – Superintendente de Bancos del Ecuador o su delegado. 2. Dr. Luis Enríquez Álvarez – Superintendente de Protección de Datos Personales o su delegado.
Sesión Nro. 26 08 de septiembre de 2025	PUNTO ÚNICO: En el marco del tratamiento del Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual, recibir en comisión general a: 1. Juan Carlos Urgiles, Gerente General de la Cooperativa de Crédito Jardín Azuayo 2. Juan Peña Aguirre Decano de la Facultad de Jurisprudencia de la Universidad de Cuenca y, 3. Polo Fabián Iñiguez Matute, expertos en temas de ciberseguridad
Sesión Nro. 28 10 de septiembre de 2025	PUNTO ÚNICO: En el marco del tratamiento del Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual, recibir en comisión general a: 1. Dr. Héctor Roberto Gordón, Máster en Seguridad Informática y, 2. Dra. Lorena Naranjo, experta en Protección de Datos y Derecho Digital.
Sesión Nro. 29 19 de septiembre de 2025	PUNTO ÚNICO: En el marco del tratamiento del Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual, recibir las observaciones de las siguientes instituciones: 1. Delegados de la Superintendencia de Economía Popular y Solidaria y,

Sesión / Fecha	Puntos Tratado
	2. Delegados de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo
Sesión Nro. 32 24 de septiembre de 2025	PUNTO ÚNICO: En el marco del tratamiento del Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual, recibir en comisión general a los siguientes invitados: 1. Delegados de la Asociación de Bancos del Ecuador y, 2. Dra. Lucia Posso Naranjo
Sesión Nro. 33 29 de septiembre de 2025	En el marco del tratamiento del Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual, 1. Recibir observaciones de los delegados del Ministerio de Defensa y, 2. Recibir en Comisión General a: 2.1. Delegados de la Asociación de Empresas de Telecomunicaciones del Ecuador ASETEL y; 2.2. Delegados de la Cámara de Innovación y Tecnología Ecuatoriana
Sesión Nro. 34 07 de octubre de 2025	En el marco del tratamiento del Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual, recibir las observaciones de las siguientes instituciones: 1. Delegados de la Contraloría General del Estado y, 2. Delegados de la Universidad de las Fuerzas Armadas ESPE: Dr. Sang Guun Yoo; Ing. Sonia Cárdenas Delgado y, Dr. Germán Rodríguez
Sesión Nro. 39 23 de octubre de 2025	PUNTO ÚNICO: En el marco del tratamiento del "Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual", recibir las observaciones de: 1. Antropólogo Gabriel Brito Collantes, experto en temas de seguridad digital
Sesión Nro. 41 28 de octubre de 2025	PUNTO ÚNICO: En el marco del tratamiento del "Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual", recibir en Comisión General las observaciones de los siguientes expertos: 1. Diego Chiza López 2. Mario Cuvero Miranda 3. Luis Cruz Rodríguez 4. Omar Durazno Ochoa 5. Deysi Espín Espín.
Sesión Nro. 42 29 de octubre de 2025	PUNTO ÚNICO: En el marco del tratamiento del "Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual", recibir en Comisión General las observaciones de los siguientes expertos: 1. Kelo Llenin González Quinde 2. Mario Alberto Mayorga Terán 3. Kevin Gilberto Jarre Barcia 4. Olmedo Xavier Narváez Montenegro 5. Ricardo Daniel Burbano Ferrín
Sesión Nro. 43 29 de octubre de 2025	PUNTO ÚNICO: En el marco del tratamiento del "Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual", recibir en Comisión General las observaciones de los siguientes expertos: 1. Ramón Joffre Moreira Pico

Sesión / Fecha	Puntos Tratado
	2. Alejandro Fabián Mero García 3. Michael Jhonny Santana Montesdeoca
Sesión Nro. 44 30 de octubre de 2025	1. En el marco del tratamiento del "Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual", recibir en Comisión General las observaciones de los siguientes expertos: a. Andrea Paulina Tenesaca b.Julio César Rosas Calderón c. Luis Alberto Urgiles Guerrero d. Ola Metodius Martin Bini e. Sara Vanesa Zambrano Vizcaíno
Sesión Nro. 46 19 de noviembre de 2025	PUNTO ÚNICO: En el marco del tratamiento del "Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual" recibir las observaciones de: a. Delegados del Ministerio de Telecomunicaciones y Sociedad de la Información.

3. BASE LEGAL PARA EL TRATAMIENTO DEL PROYECTO DE LEY

Constitución de la República del Ecuador

Art. 120.- La Asamblea Nacional tendrá las siguientes atribuciones y deberes, además de las que determine la ley:

"(...) 6. Expedir, codificar, reformar y derogar las leyes, e interpretarlas con carácter generalmente obligatorio.

Art. 136.- Los proyectos de ley deberán referirse a una sola materia y serán presentados a la Presidenta o Presidente de la Asamblea Nacional con la suficiente exposición de motivos, el articulado que se proponga y la expresión clara de los artículos que con la nueva ley se derogarían o se reformarían. Si el proyecto no reúne estos requisitos no se tramitará.

Art. 137.- El proyecto de ley será sometido a dos debates. La Presidenta o Presidente de la Asamblea Nacional, dentro de los plazos que establezca la ley, ordenará que se distribuya el proyecto a los miembros de la Asamblea y se difunda públicamente su extracto, y enviará el proyecto a la comisión que corresponda, que iniciará su respectivo conocimiento y trámite.

Las ciudadanas y los ciudadanos que tengan interés en la aprobación del proyecto de ley, o que consideren que sus derechos puedan ser afectados por su expedición, podrán acudir ante la comisión y exponer sus argumentos.

Aprobado el proyecto de ley, la Asamblea lo enviará a la Presidenta o Presidente de la República para que lo sancione u objete de forma fundamentada. Sancionado el proyecto de ley o de no haber objeciones dentro del plazo de treinta días posteriores a su recepción

por parte de la Presidenta o Presidente de la República, se promulgará la ley, y se publicará en el Registro Oficial.

Ley Orgánica de la Función Legislativa

Art. 61.- Del segundo debate.- La comisión especializada analizará y de ser el caso, recogerá las observaciones efectuadas al proyecto de Ley, en el primer debate.

Dentro del plazo máximo de noventa días, contado a partir del cierre de la sesión del Pleno, la comisión especializada presentará a la Presidenta o al Presidente de la Asamblea Nacional el informe para segundo debate.

La comisión especializada, atendiendo a la naturaleza y complejidad del proyecto de ley, 1podrá pedir justificadamente a la Presidenta o al Presidente de la Asamblea Nacional, por una sola vez, la prórroga que considere necesaria para presentar el informe correspondiente. La Presidenta o el Presidente de la Asamblea Nacional determinará si concede o no la prórroga, así como el plazo de la misma.

La Presidenta o el Presidente, recibido el informe para segundo debate, ordenará por Secretaría General de la Asamblea Nacional, la distribución del informe a las y los asambleístas.

El segundo debate se desarrollará, previa convocatoria de la Presidenta o del Presidente de la Asamblea Nacional, en una sola sesión, en un plazo máximo de seis meses desde la recepción del informe.

En el caso de negarse el informe de mayoría, el Pleno de la Asamblea, por decisión de la mayoría simple de sus integrantes, podrá decidir la votación del o los informes de minoría.

Durante el segundo debate el o la ponente recogerá las observaciones realizadas por el Pleno.

En caso de que el proyecto amerite cambios, la o el ponente solicitará a la Presidenta o al Presidente de la Asamblea Nacional, la suspensión del punto del orden del día, a fin de que la comisión analice la incorporación de los cambios sugeridos. Para este efecto, la Presidenta o el Presidente de la comisión respectiva, convocará a la comisión para que en una sola sesión, analice y apruebe el texto final de votación sugerido, el mismo que será entregado al Pleno de la Asamblea Nacional, en el plazo máximo de ocho días desde el pedido de suspensión del punto del orden del día.

Cuando existan cambios en el texto final para votación, el ponente tendrá la obligación de indicar los mismos, previo a la votación.

En el caso de que la comisión no tenga mayoría para aprobar o improbar los cambios en el plazo determinado de ocho días, la o el ponente tendrá la potestad de presentar el texto de votación al Pleno de la Asamblea Nacional.

Si el texto aprobado por la comisión y que incorpora las observaciones del segundo debate no cuenta con los votos necesarios para su aprobación en el Pleno de la Asamblea

Nacional, la o el ponente podrá realizar los ajustes pertinentes y mocionar ante el Pleno de la Asamblea Nacional la aprobación del proyecto de Ley con el nuevo texto, indicando las modificaciones realizadas.

Agotado el segundo debate, la votación del texto final del proyecto de ley no podrá exceder el plazo de sesenta días. Se podrá mocionar la aprobación del texto íntegro de la ley, por secciones o artículos.
Con el voto favorable de la mayoría absoluta, el Pleno de la Asamblea Nacional, podrá archivar el proyecto de ley.

Art. 63.- De la remisión del proyecto de ley a la Presidenta o Presidente de la República.- Como tiempo máximo, a los dos días hábiles siguientes luego de la aprobación del proyecto de ley, la Presidenta o Presidente de la Asamblea Nacional lo enviará a la Presidenta o Presidente de la República para que lo sancione u objete de forma fundamentada. Sancionado el proyecto de ley o de no haber objeciones dentro del plazo máximo de treinta días posteriores a su recepción por parte de la Presidenta o Presidente de la República, se promulgará la ley y se publicará en el Registro Oficial.

Reglamento de las Comisiones Especializadas Permanentes y Ocasionales

Art. 8.- Funciones del pleno de la comisión especializada permanente y ocasional. Sin perjuicio de las funciones previstas en el artículo 26 de la Ley Orgánica de la Función Legislativa, el pleno de la comisión especializada permanente y ocasional deberá:

"(…) 8. Discutir, elaborar y aprobar con el voto favorable de la mayoría absoluta, los informes de los proyectos de ley, previo a ser sometidos a conocimiento y aprobación del Pleno de la Asamblea Nacional. Para la aprobación del informe, en caso de empate, la presidenta o el presidente de la comisión especializada tendrá voto dirimente;

Art. 30.- Informes aprobados por la Comisión. Los informes que sean aprobados por las comisiones especializadas permanentes y ocasionales sobre los proyectos de ley, los acuerdos, resoluciones y más actos legislativos, según lo establecido en la Ley Orgánica de la Función Legislativa, contendrán como mínimo los siguientes parámetros, según el formato de Informe anexo al presente Reglamento. "(...)"

Art. 32.- Envío a la Presidencia de la Asamblea Nacional. Los informes de los proyectos de ley, acuerdos, resoluciones y demás actos legislativos deberán ser remitidos a la Presidenta o Presidente de la Asamblea Nacional en el formato de memorando que contendrá como mínimo lo siguiente:

1. Numeración del documento;
2. Fecha del documento;
3. Nombre de la presidenta o presidente de la comisión especializada correspondiente;
4. Nombre del proyecto de ley, acuerdo, resolución o demás actos legislativos;
5. Nombre de la/ o el asambleísta proponente; y,
6. Detalle de la votación realizada en la comisión.

Los formatos de actas, informes y memorando detallado en este Artículo, estarán disponibles de forma digital en la intranet institucional.

4. ANÁLISIS Y RAZONAMIENTO

1. Consideraciones generales sobre la necesidad de la reforma

La Comisión, una vez concluido el proceso de recepción de observaciones institucionales, sectoriales, académicas y ciudadanas, procedió a evaluar y sistematizar todos los aportes recibidos tras la aprobación del informe para primer debate. En este marco, se constató que la versión inicial del articulado requería un desarrollo más profundo para asegurar coherencia normativa, precisión técnica y alineación con las mejores prácticas internacionales en gestión de riesgos digitales, protección de infraestructura crítica y gobernanza de la seguridad digital. Asimismo, se advirtió la necesidad de incorporar instrumentos técnicos específicos - como el Catálogo Nacional de Servicios Esenciales e Infraestructura Crítica Digital y un régimen de notificación de incidentes basado en estándares internacionales - que permitan operacionalizar un enfoque de ciberseguridad basado en riesgo.

La acelerada digitalización del Estado ecuatoriano, junto con la creciente dependencia de sistemas tecnológicos para la prestación de servicios esenciales, ha producido un incremento sustancial de la superficie de exposición del país frente a ciberataques, fallas técnicas, incidentes internos y eventos que comprometen la continuidad operativa de instituciones públicas y privadas. Estos riesgos, como se evidenció en múltiples comparecencias, no solo afectan el funcionamiento administrativo del Estado, sino que pueden escalar hacia afectaciones económicas, sociales y de seguridad nacional.

En ausencia de un marco normativo uniforme, integrado y actualizado en materia de ciberseguridad, el país se enfrenta a vacíos regulatorios que dificultan la prevención, detección, respuesta y recuperación frente a incidentes digitales. Esto limita la capacidad estatal de coordinar políticas públicas, ordenar institucionalmente la gestión de riesgos, articular la relación con los sectores regulados y no regulados y proteger adecuadamente la infraestructura crítica nacional. El carácter transversal del riesgo digital exige una arquitectura normativa clara y operativa que oriente a todos los actores en el cumplimiento de estándares mínimos y procedimientos de gestión de incidentes. La presente propuesta busca superar estos vacíos mediante la definición de principios rectores, la identificación priorizada de servicios esenciales, la implementación de procesos de notificación oportuna y la asignación de obligaciones diferenciadas según el nivel de riesgo.

El análisis realizado por la Comisión evidencia la necesidad de consolidar un cuerpo normativo que, sin alterar la estructura de la Ley Orgánica para la Transformación Digital y Audiovisual, incorpore un esquema estructurado de ciberseguridad que integre principios, competencias, obligaciones, mecanismos de notificación, procesos de coordinación institucional, instrumentos de gobernanza y un régimen sancionador proporcional y basado en riesgo. Este enfoque es el que se materializa en la presente propuesta para segundo debate.

Nota de contexto - Eventos globales de interrupción digital (2025).

En noviembre de 2025 se registraron eventos de alcance global que evidenciaron la magnitud y la inmediatez de los riesgos asociados a la infraestructura digital. El 18 de noviembre, la empresa Cloudflare[1] reportó fallas en su red global, afectando temporalmente servicios como X (antes Twitter), League of Legends, Spotify y Amazon. Este episodio ocurrió menos de un mes después de que Amazon Web Services (AWS) [2] experimentara una interrupción significativa que impactó servicios gubernamentales, financieros y comerciales en distintos países. Estos eventos reflejan la interdependencia técnica existente entre servicios locales y proveedores globales de infraestructura digital y muestran que incidentes generados fuera del territorio nacional pueden producir efectos indirectos en la continuidad de servicios públicos y privados en el país.

Nota de contexto – Panorama nacional de amenazas cibernéticas.

Ecuador registró más de 12 millones de ciberataques en 2023, con un incremento estimado del 30% en 2024, situándose entre los países más atacados de América Latina[3] [4]. En febrero de 2025, la Asamblea Nacional sufrió dos intentos de acceso no autorizado a sistemas institucionales[5], mientras que en abril de 2024 el Municipio de Quito enfrentó un ataque de ransomware que comprometió cerca del 20% de su base de datos[6]. En julio de 2025, el ECU-CERT alertó sobre la presencia activa del grupo Interlock Ransomware en el país[7]. Estos incidentes evidencian la necesidad urgente de consolidar un sistema nacional de ciberseguridad robusto, interoperable y basado en riesgo.

2. Justificación de la vía normativa y del marco de integración

La Comisión ratifica la decisión inicial de integrar la regulación de la ciberseguridad dentro de la Ley Orgánica para la Transformación Digital y Audiovisual, en lugar de crear un cuerpo normativo autónomo. Este criterio responde a razones de técnica legislativa y coherencia institucional.

La ciberseguridad constituye un componente estructural del proceso de transformación digital, no un ámbito ajeno o paralelo. En los modelos comparados (Unión Europea – NIS2, España, Colombia, Chile, OEA/CICTE), la seguridad digital se establece como una condición habilitante para la modernización tecnológica del Estado, integrada a la gobernanza digital y estrechamente asociada a la protección de infraestructura crítica, servicios esenciales y datos personales.

Evitar dispersión normativa.

La creación de una ley independiente podría generar duplicidad de funciones, tensiones competenciales y superposición con marcos regulatorios existentes, particularmente en materia de telecomunicaciones, protección de datos personales, defensa nacional, banca y sistema financiero, energía, salud y educación.

[1] https://www.nytimes.com/es/2025/11/18/espanol/negocios/caida-internet-cloudfare.html
[2] https://www.bbc.com/mundo/articles/cge57zllpnro
[3] https://www.telefonica.com.ec/security-forum-de-movistar-empresas-analizo-el-escenario-y-tendencias-de-ciberseguridad-en-el-pais/
[4] https://www.saphirtek.com/blogs/ciberataques-en-ecuador-alarmante-aumento-en-2024
[5] https://therecord.media/ecuador-national-assembly-cyberattack
[6] https://www.swissinfo.ch/spa/el-municipio-de-quito-víctima-de-ciberataque-que-afectó-el-15-de-sus-datos/47525602
[7] https://www.ecucert.gob.ec/wp-content/uploads/2025/07/AL-2025-036-Interlock-Ransomware.pdf

Respetar la iniciativa legislativa establecida en el artículo 135 de la Constitución, que restringe la posibilidad de crear nuevas institucionalidades orgánicas cuando no se cuenta con iniciativa exclusiva del Presidente. La integración dentro de la LOTDA viabiliza un marco funcional sin generar estructuras adicionales y permite consolidar, en un solo cuerpo, la rectoría en transformación digital y ciberseguridad.

Asegurar la sostenibilidad fiscal prevista en el artículo 287 constitucional.

El proyecto optimiza las capacidades existentes, consolidando roles y evitando creación de burocracia.

Alineación con la Política Pública para la Transformación Digital 2025–2030 y con la Política Nacional de Ciberseguridad.

La integración normativa permite armonizar rectoría, planificación, implementación y control en un único marco articulador, evitando fragmentación institucional y garantizando continuidad entre la política pública y el diseño legal.

En consecuencia, se sostiene la vía reformatoria como la ruta más adecuada desde el punto de vista constitucional, fiscal y técnico.

3. Marco constitucional y distribución de competencias

La Comisión analizó detenidamente la conformidad del proyecto con la estructura constitucional vigente.

Además resolvió reforzar el texto normativo para evitar conflictos competenciales, garantizando que:

- El ente rector ejerza rectoría, planificación y coordinación, sin sustituir la fiscalización sectorial;
- La Autoridad de Protección de Datos Personales conserve plena autonomía en materia de tratamiento de datos;
- Los órganos constitucionalmente autónomos (CNE, Contraloría, Banco Central, Fiscalía, Asamblea Nacional, Función Judicial) mantengan independencia técnica, operativa y normativa en materia de seguridad informática;
- El régimen sancionador se aplique solo a sectores sin órgano especializado, mediante subsidiariedad;
- El Ministerio de Defensa participe solo en los aspectos relacionados con escalamiento de incidentes que afecten seguridad nacional, respetando su función constitucional; y,
- Se respeten los principios de especialidad y non bis in ídem, evitando superposición sancionadora entre el ente rector y los órganos de control especializados.

4. Construcción del régimen de ciberseguridad y razonamiento por capítulos

4.1 Principios y coordinación

Se incorporó un catálogo detallado de principios inspirados en marcos internacionales (NIS2, ISO/IEC 27000, NIST) para orientar la actuación de instituciones, prestadores digitales y operadores de infraestructura crítica. La inclusión de principios como resiliencia, neutralidad tecnológica, proporcionalidad y privacidad desde el diseño asegura la compatibilidad con estándares globales y con la LOPDP. Estos principios constituyen el marco interpretativo general del sistema, orientan la gestión basada en riesgos y guían la adopción de medidas técnicas, organizativas y administrativas en todos los sectores.

En atención a la naturaleza evolutiva de las amenazas digitales, la Comisión incorporó el principio de adaptabilidad tecnológica, mediante el cual se reconoce que los mecanismos de seguridad deben ajustarse dinámicamente a los cambios tecnológicos que puedan comprometer la eficacia de los estándares vigentes. La computación cuántica constituye uno de los principales vectores emergentes de riesgo, pues tiene el potencial de vulnerar esquemas criptográficos ampliamente usados en la administración pública y en el sector privado. La incorporación de este principio garantiza que el ente rector mantenga un proceso continuo de evaluación técnica y actualización normativa, orientado hacia la adopción de mecanismos criptográficos resilientes y estándares internacionales aprobados por organismos como NIST, ETSI o ENISA. Esta previsión normativa fortalece la resiliencia del país frente a amenazas futuras y asegura que el marco regulatorio no pierda vigencia frente al avance científico y tecnológico.

La coordinación estratégica y operativa se define con criterios diferenciados para evitar duplicidad regulatoria, respetar la autonomía de órganos de control especializado y consolidar un modelo de gobernanza nacional coherente con la política pública vigente. El ente rector asume un rol de articulación y dirección técnica, mientras que los órganos sectoriales conservan sus competencias regulatorias y sancionadoras, en un esquema de cooperación y no de sustitución.

Como complemento al marco de principios, la Comisión destaca que la ciberseguridad no se limita a la adopción de medidas técnicas, sino que exige el fortalecimiento de capacidades humanas y sociales. En este sentido, las reformas a la Ley Orgánica de Educación Intercultural (LOEI) incorporadas en este proyecto representan uno de los pilares más relevantes de la arquitectura nacional de seguridad digital, al promover que la ciudadanía desarrolle desde etapas tempranas competencias de alfabetización digital, pensamiento crítico, autocuidado en línea y hábitos de higiene digital.

4.2 Gestión de incidentes y notificación

Se estableció un mecanismo claro de reporte de incidentes, basado en ventanas de tiempo razonables (72 horas), adecuados a estándares internacionales. Este plazo permite equilibrar la necesidad de contar con información temprana para activar capacidades nacionales de respuesta con la complejidad técnica que implica la detección y análisis preliminar de incidentes sofisticados, en línea con prácticas comparadas como la Directiva NIS2. La notificación diferenciada para órganos especializados (como superintendencias) respeta su rol sectorial y evita sobrecarga institucional.

Se incluyó una garantía de no utilización automática de la notificación como prueba de negligencia, promoviendo cultura de reporte voluntario y oportuno, y reforzando la confianza entre el sector público, el sector privado y el ente rector para la gestión colaborativa de incidentes.

Nota de contexto – Consecuencias de la falta de notificación temprana.

Se identificaron casos internacionales donde la falta de reporte oportuno agravó considerablemente los daños generados por incidentes de ciberseguridad. Entre ellos destacan el caso Equifax (2017), cuya brecha afectó a más de 147 millones de personas y fue ocultada durante meses[8]; el caso Uber (revelado en 2022), donde una intrusión permaneció encubierta durante dos años[9]; y el ataque a SolarWinds (2020), cuya detección tardía permitió la propagación del compromiso a múltiples agencias gubernamentales y empresas estratégicas en distintos países[10]. Estos antecedentes confirman la importancia de establecer plazos uniformes de notificación y mecanismos claros de reporte que permitan activar capacidades de respuesta coordinada.

4.3 Prestadores de servicios digitales y sector privado

La Comisión, tras analizar las observaciones recibidas y el informe técnico remitido por el órgano rector, considera necesario precisar el rol de los prestadores de servicios digitales (PSD) dentro del sistema nacional de ciberseguridad. Los PSD no operan servicios esenciales ni infraestructura crítica digital, sino que forman parte de la cadena de suministro tecnológico, por lo que sus obligaciones deben situarse en el marco del principio de responsabilidad compartida. En consecuencia, la Comisión estima que no corresponde establecer una clasificación jurídica de PSD en niveles de criticidad, pues ello no responde a estándares internacionales y podría generar paralelismos regulatorios innecesarios.

Las cargas regulatorias y las obligaciones de reporte deben recaer en quienes operan servicios esenciales y en los operadores de infraestructura crítica digital, mientras que las obligaciones de los PSD deben ejecutarse principalmente mediante mecanismos contractuales que aseguren la adopción de medidas técnicas y organizativas basadas en estándares internacionales. Este enfoque mantiene la coherencia del sistema, evita sobrerregulación, y garantiza una colaboración efectiva entre operadores esenciales y sus proveedores tecnológicos.

El artículo sobre hacking ético y pruebas de vulnerabilidad establece salvaguardas de consentimiento, finalidad legítima, protección de datos y reporte, evitando criminalización de actividades autorizadas y profesionalizadas. De esta manera, se habilita jurídicamente la realización de pruebas de penetración y evaluaciones de seguridad en entornos controlados, bajo responsabilidad de personas y entidades calificadas, con el objetivo de identificar y remediar vulnerabilidades antes de que sean explotadas por actores maliciosos.

De manera complementaria, la Comisión reconoce que ninguna infraestructura o sistema es plenamente seguro si los usuarios carecen de las competencias básicas para identificar

[8] https://www.univision.com/noticias/delitos-ciberneticos/un-ciberataque-a-la-gigante-medidora-de-credito-equifax-pudo-haber-afectado-a-143-millones-de-personas
[9] https://www.semana.com/uber-oculto-hackeo-masivo-que-afecto-57-millones-de-usuarios/252605/
[10] https://www.fortinet.com/lat/resources/cyberglossary/solarwinds-cyber-attack

riesgos, evitar conductas inseguras y actuar frente a amenazas. Por ello, las reformas a la LOEI contribuyen a cerrar la brecha entre la dimensión técnica de la ciberseguridad y la dimensión humana, formando nuevas generaciones con criterios de prevención, seguridad y comportamiento responsable en entornos digitales.

Asimismo, se incorporó una atribución específica del ente rector para establecer lineamientos técnicos de actualización criptográfica, con el fin de mitigar riesgos emergentes relacionados con nuevas capacidades tecnológicas, incluyendo la computación cuántica. Esta atribución permitirá orientar la transición hacia algoritmos robustos y mecanismos criptográficos avanzados, fomentando la interoperabilidad, la seguridad y la protección de sistemas de alto impacto.

Nota de contexto – Importancia del hacking ético en la seguridad global.

Casos relevantes donde actividades de investigación autorizada permitieron prevenir incidentes de alto impacto. La vulnerabilidad global conocida como "Heartbleed", descubierta en 2014 por especialistas independientes, evidenció la importancia de contar con mecanismos que habiliten pruebas controladas de seguridad [11] . Asimismo, múltiples programas de *bug bounty* implementados por empresas tecnológicas han permitido identificar fallas críticas antes de que puedan ser explotadas, evitando afectaciones potencialmente devastadoras en servicios públicos y privados. Estos ejemplos fundamentan la habilitación normativa del hacking ético en este proyecto.

Nota de contexto – Computación cuántica y transición hacia criptografía post-cuántica (NIST PQC)

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) conduce, desde 2016, un proceso internacional de evaluación y estandarización de algoritmos criptográficos resistentes a capacidades cuánticas, conocido como Post-Quantum Cryptography Standardization Project (PQC)[12]. Este proceso busca seleccionar mecanismos de cifrado y firma digital que permanezcan seguros incluso frente a adversarios que dispongan de computadoras cuánticas de gran escala.

En los últimos años se han logrado avances significativos en la construcción de dispositivos cuánticos capaces de resolver problemas matemáticos que sustentan los criptosistemas de clave pública actualmente utilizados, como RSA, Diffie–Hellman y la criptografía de curva elíptica. Una computadora cuántica a gran escala tendría la capacidad de vulnerar estos mecanismos mediante algoritmos como el de Shor, comprometiendo la confidencialidad, integridad y autenticidad de las comunicaciones digitales, así como la infraestructura crítica que depende de ellos.

La criptografía post-cuántica tiene como objetivo desarrollar sistemas criptográficos seguros frente a capacidades cuánticas y clásicas, que puedan integrarse en las redes y protocolos existentes sin alterar su funcionamiento. Dado que la transición hacia nuevos estándares de seguridad suele requerir varios años, el NIST y otros organismos internacionales —como ENISA y ETSI— recomiendan que los Estados inicien procesos de adaptación temprana para evitar vulnerabilidades futuras.

La incorporación en esta ley del principio de adaptabilidad tecnológica y de la atribución del ente rector para actualizar mecanismos criptográficos se alinea directamente con estas recomendaciones internacionales y permite al Ecuador anticiparse a los riesgos emergentes derivados del avance de la computación cuántica, estableciendo un marco normativo para una transición oportuna, ordenada y basada en riesgo hacia estándares criptográficos resilientes.

[11] https://heartbleed.com

[12] https://csrc-nist-gov.translate.goog/projects/post-quantum-cryptography?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

4.4 Infraestructura crítica digital

Se definió un marco robusto para identificar, clasificar y proteger infraestructura crítica digital, elemento central de la seguridad nacional y de la continuidad de servicios esenciales. En este contexto, el Catálogo Nacional de Servicios Esenciales e Infraestructura Crítica Digital se configura como el instrumento técnico mediante el cual se priorizan activos, se ordenan interdependencias sectoriales y se orientan las capacidades de protección y respuesta, siguiendo criterios objetivos y un enfoque basado en riesgo. La Comisión ajustó la redacción para evitar interferencias con autoridades sectoriales, limitando la intervención del ente rector a criterios normativos generales.

Nota de contexto – Ataques a infraestructura crítica.

Incidentes que dejaron en evidencia la vulnerabilidad de infraestructura crítica en distintos países. Entre ellos destacan el ataque al sistema hospitalario de Irlanda (2021), que paralizó durante semanas la atención médica y obligó a activar medidas extraordinarias[13]; los ataques de ransomware contra hospitales en Alemania, que comprometieron la disponibilidad de servicios de emergencia[14]; y la intrusión al sistema financiero internacional SWIFT (2016), que afectó procesos de transferencia a escala global[15]. Estos casos demuestran que la protección de servicios esenciales requiere un esquema de priorización y gestión basado en riesgos objetivos.

4.5 Gobernanza y cooperación internacional

El proyecto fortalece el Comité Nacional de Ciberseguridad como instancia estratégica, en coherencia con el Decreto 464. Se aclara que el reglamento determinará su estructura interna, sin generar órganos nuevos más allá de los previstos. Esta instancia actúa como espacio de coordinación de alto nivel para la adopción de lineamientos, la articulación interinstitucional y la evaluación de la implementación de la política nacional de ciberseguridad.

Asimismo, se promueve cooperación en redes globales (CSIRT, CERT, FIRST) y con organismos multilaterales, alineando al país con esfuerzos internacionales en prevención y contención de amenazas transnacionales. La participación activa en estas redes permite acceso a alertas tempranas, intercambio de información técnica relevante y coordinación en la respuesta frente a incidentes de naturaleza transfronteriza, reforzando las capacidades nacionales más allá de las fronteras físicas del Estado.

Nota de contexto – Naturaleza transnacional de las amenazas.

Incidentes de ransomware y ciberataques con impacto global, como WannaCry (2017), que afectó a hospitales y entidades públicas en más de 150 países[16]; NotPetya (2017), que paralizó puertos, aerolíneas y cadenas logísticas en distintos continentes[17]; y el ataque contra la red satelital Viasat (2022), que

[13] https://www.abc.es/internacional/abci-ciberataque-obliga-sistema-salud-irlanda-cerrar-sistema-informatico-y-suspender-consultas-202105141055_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Finternacional%2Fabci-ciberataque-obliga-sistema-salud-irlanda-cerrar-sistema-informatico-y-suspender-consultas-202105141055_noticia.html

[14] https://elpais.com/internacional/2020-10-03/ciberataque-a-un-hospital-aleman-en-tiempos-de-pandemia.html

[15] https://www-nytimes-com.translate.goog/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

[16] https://www.cloudflare.com/es-es/learning/security/ransomware/wannacry-ransomware/

[17] https://www.cloudflare.com/es-es/learning/security/ransomware/petya-notpetya-ransomware/

perturbó comunicaciones críticas durante eventos geopolíticos[18]. Estos hechos evidencian que las amenazas cibernéticas trascienden fronteras y requieren cooperación activa con redes internacionales de CSIRT y organismos multilaterales.

4.6 Régimen administrativo sancionador

La Comisión incorporó un régimen de sanciones basado en:

- Gradualidad,
- Riesgo sistémico,
- Criticidad del servicio,
- Conducta del infractor.

Se garantiza el principio non bis in ídem y se reconoce la competencia plena de los órganos especializados (superintendencias). El ente rector solo sancionará en sectores sin regulación previa, bajo enfoque preventivo y subsidiario. De esta forma, el régimen sancionador se integra al sistema general del COA, respetando las garantías del debido proceso, evitando duplicidades sancionadoras y privilegiando la corrección temprana de incumplimientos a través de medidas preventivas y correctivas antes que meramente punitivas.

4.7 Educación, higiene digital y fortalecimiento de capacidades humanas

Uno de los elementos más trascendentes del proyecto, y que posiciona a esta reforma por encima de modelos comparados, es la incorporación de ajustes a la Ley Orgánica de Educación Intercultural (LOEI) para integrar de manera estructural la alfabetización digital, la seguridad digital y la higiene digital en todos los niveles del sistema educativo.

La Comisión considera que la ciberseguridad, para ser efectiva, debe incorporar una dimensión humana que complemente la infraestructura tecnológica, los sistemas de gestión y la gobernanza institucional. La experiencia internacional demuestra que los comportamientos inseguros de los usuarios, el desconocimiento de riesgos y la falta de hábitos digitales saludables son factores tan críticos como las vulnerabilidades técnicas en sistemas o redes.

Por ello, la reforma a la LOEI habilita la inclusión de contenidos curriculares específicos sobre:

- Habilidades de autocuidado digital;
- Protección de datos personales y privacidad;
- Uso ético y responsable de tecnologías;
- Pensamiento crítico frente a contenidos digitales;
- Prevención del acoso, violencia digital y manipulación algorítmica;
- Identificación temprana de señales de riesgo;
- Higiene digital y reducción de exposición innecesaria.

[18] https://www-bbc-com.translate.goog/news/technology-61396331?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc&_x_tr_hist=true

Esta medida expresa la convicción de la Comisión de que la seguridad digital del Estado depende tanto de capacidades tecnológicas e institucionales como de la formación de ciudadanía digital consciente, crítica, informada y resiliente. La incorporación de estos contenidos en la LOEI permite institucionalizar la prevención como política pública, generando impactos sostenibles a largo plazo en la cultura digital del país.

Nota de contexto – Incidentes originados en fallas humanas.

Diversos estudios internacionales señalan que una proporción significativa de los incidentes de ciberseguridad - estimada en más del 90% - tiene su origen en errores humanos[19], tales como configuraciones incorrectas, descuidos operativos, uso de contraseñas débiles o manipulación inadvertida de sistemas y datos. Estos hallazgos resaltan la importancia del componente humano en la seguridad digital y la necesidad de fortalecer capacidades, hábitos de higiene digital y procesos internos de prevención en las organizaciones.

Nota de contexto – Riesgos digitales en niños, niñas y adolescentes

Según UNICEF[20], el 71% de los jóvenes entre 15 y 24 años están conectados a internet a nivel mundial, y cada vez más niños acceden a la tecnología desde edades tempranas. El organismo señala que los menores de 18 años representan aproximadamente uno de cada tres usuarios de internet en el mundo, y que en diversos países los niños menores de 15 años tienen una probabilidad similar de conexión que los adultos mayores de 25. El uso extendido de teléfonos inteligentes ha impulsado una "cultura del dormitorio", caracterizada por un acceso más personal, privado y menos supervisado. Estas dinámicas incrementan la exposición de niños y adolescentes a riesgos como el ciberacoso, el grooming y la desinformación, en un contexto donde los sistemas educativos aún no están plenamente preparados para ofrecer protección integral.

Las Naciones Unidas[21] advierten que los jóvenes que interactúan en redes sociales o plataformas de mensajería instantánea pueden ser objeto de ciberacoso y otras formas de violencia digital. En estudios realizados en 30 países, más de un tercio de los jóvenes reportaron haber sufrido acoso en línea y uno de cada cinco afirmó haber faltado a la escuela a causa de ello. La exposición a contenidos violentos, discursos de odio o incitaciones a la autolesión constituye un riesgo adicional, amplificado por la omnipresencia del entorno digital y la dificultad de los menores para desconectarse de él.

La UNESCO[22] subraya la importancia de incorporar la alfabetización y la seguridad digital en los sistemas educativos para que los estudiantes desarrollen competencias que les permitan navegar de forma segura en internet. La implementación de políticas educativas de seguridad digital facilita que docentes y centros educativos identifiquen riesgos, intervengan ante casos de violencia digital y promuevan entornos de aprendizaje seguros e inclusivos. Este enfoque refuerza la capacidad de los estudiantes para adoptar prácticas de autocuidado y respeto en entornos digitales.

La Convención sobre los Derechos del Niño, ratificada por el Ecuador, exige a los Estados proteger a los menores en todas las esferas de su vida, incluidos los entornos digitales. El Comité de los Derechos del Niño de la ONU[23] ha emitido directrices que instan a los Estados a fortalecer la seguridad digital de los menores y a garantizar que los sistemas educativos cuenten con capacidades para prevenir, identificar

[19] https://blogs.uoc.edu/informatica/es/factor-humano-en-la-ciberseguridad/ https://www.incibe.es/ciudadania/blog/sabias-que-el-95-de-las-incidencias-en-ciberseguridad-se-deben-errores

[20] Estado Mundial de la Infancia 2017. Niños en un mundo digital. https://www.unicef.org/media/48611/file#:~:text=Los%20niños%20y%20adolescentes%20menores,edades%20cada%20vez%20más%20tempranas.

[21] La seguridad de la infancia y la juventud en la red. https://www.un.org/es/global-issues/child-and-youth-safety-online

[22] Qué debe saber sobre la alfabetización. https://www.unesco.org/es/literacy/need-know

[23] Observación general núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital. https://www.plataformadeinfancia.org/wp-content/uploads/2021/09/observacion-general-25-relativa-a-los-derechos-de-los-ninos-en-relacion-con-el-entorno-digital.pdf

e intervenir frente a riesgos en línea. Estas obligaciones constituyen un marco internacional que orienta la adopción de medidas de protección en el sistema educativo nacional.

5. Observaciones recibidas y ajustes realizados

Durante el proceso posterior al primer debate, la Comisión recibió y analizó un conjunto amplio de observaciones provenientes de instituciones públicas, órganos de control especializado, sectores regulados, academia, expertos independientes y actores relevantes de la industria tecnológica. En particular, se consideraron los aportes remitidos por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), la Corporación Nacional de Telecomunicaciones (CNT EP), la Asociación de Bancos Privados del Ecuador (ASOBANCA), la Superintendencia de Economía Popular y Solidaria (SEPS), la Fiscalía General del Estado, la Contraloría General del Estado, instituciones académicas y centros de investigación, así como empresas tecnológicas y prestadores de servicios digitales con alta relevancia operativa para servicios esenciales. La consolidación de las reformas a la LOEI fue destacada de manera reiterada por instituciones académicas, centros de investigación y expertos en psicología, educación digital y derechos de la niñez, quienes subrayaron que la seguridad digital es, ante todo, una competencia humana y social. La Comisión acogió plenamente estas observaciones, integrando de manera estructural la educación digital como parte esencial de la norma.

La Comisión incorporó en el artículo 20-B el principio de adaptabilidad tecnológica y, en el artículo 7-A, una atribución específica para actualizar los mecanismos criptográficos del Estado y de los prestadores de servicios digitales. Estos ajustes responden a observaciones técnicas recibidas por el sector académico, organizaciones especializadas en seguridad, y actores de la industria tecnológica, quienes advirtieron la necesidad de anticipar los riesgos derivados de la computación cuántica y garantizar que los sistemas nacionales mantengan niveles adecuados de protección frente a amenazas emergentes. Esta previsión normativa alinea al país con procesos internacionales de estandarización criptográfica, particularmente el programa de Criptografía Post-Cuántica del NIST[24], consolidando un enfoque anticipatorio y basado en riesgo.

La Comisión arguye en esta fase que las modificaciones más relevantes responden a:

- Necesidad de claridad competencial.
- Evitar duplicidad normativa con la LOPDP.
- Ajustar definiciones y principios para asegurar armonización interinstitucional.
- Reforzar la matriz de responsabilidades para el sector privado.
- Incorporar mecanismos de verificación técnica solo en sectores no regulados.
- Garantizar sostenibilidad fiscal de la reforma.
- Incorporar estándares internacionales de manera neutral.
- Integrar instrumentos técnicos específicos - como el catálogo nacional de servicios esenciales e infraestructura crítica digital, el régimen de notificación de incidentes y la habilitación del hacking ético - que fueron sugeridos por diversos

[24] https://csrc-nist-gov.translate.goog/projects/post-quantum-cryptography?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

actores públicos y privados como buenas prácticas necesarias para un sistema moderno de ciberseguridad.

Asimismo, se incorporaron reformas adicionales para asegurar coherencia transversal del sistema jurídico con la noción de seguridad digital, educación en higiene digital, cooperación pública y protección de infraestructura crítica.

6. Evaluación constitucional, fiscal y regulatoria

La Comisión concluye que:

- No se crean nuevas instituciones, cumpliendo la exigencia de iniciativa del art. 135.
- La rectoría se mantiene dentro del marco previsto por la LOTDA, sin expansión indebida.
- El proyecto fortalece derechos fundamentales, especialmente aquellos vinculados a seguridad digital, protección de datos personales, acceso a servicios esenciales y confianza ciudadana.
- El régimen sancionador respeta el COA, incorporando garantías de debido proceso y separación de funciones.

Desde una perspectiva de gestión regulatoria, la Comisión considera que la presente versión:

- Reduce costos de cumplimiento.
- Estabiliza reglas técnicas.
- Previene costos asociados a incidentes críticos.
- Y fomenta un entorno seguro para la innovación, al proporcionar certeza jurídica, reglas previsibles y un marco de obligaciones graduadas según el nivel de riesgo y la criticidad de los servicios involucrados.

5. CONCLUSIONES Y RECOMENDACIONES DEL INFORME

Conclusión general

El texto normativo que se propone para segundo debate constituye una arquitectura moderna, técnicamente fundada y constitucionalmente compatible para robustecer la ciberseguridad nacional, articular un modelo coherente de gobernanza digital, proteger infraestructura crítica y garantizar continuidad de servicios esenciales. Integra, además, los principales estándares y buenas prácticas internacionales, instrumentos técnicos de priorización de riesgos y mecanismos de coordinación y cooperación que permiten al país afrontar de mejor manera la naturaleza transnacional y evolutiva de las amenazas digitales. La Comisión resalta especialmente que, mediante las reformas a la LOEI, el proyecto incorpora la dimensión humana de la ciberseguridad, fortaleciendo la capacidad preventiva del Estado y asegurando que la educación digital se convierta en un eje fundamental de la resiliencia nacional.

Recomendación

La Comisión recomienda su aprobación en segundo debate al Pleno de la Asamblea Nacional.

6. RESOLUCIÓN Y DETALLE DE LA VOTACION DEL INFORME

Por las motivaciones constitucionales y legales expuestas en el presente informe, así como las señaladas en las sesiones realizadas por la Comisión Especializada Permanente De Soberanía, Integración, y Seguridad Integral, **RESUELVE** aprobar el presente INFORME PARA SEGUNDO DEBATE DEL **"PROYECTO DE LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD"**, con SIETE (7) votos a favor, CERO (0) en contra, TRES (3) abstenciones de las y los asambleístas presentes.

7. ASAMBLEÍSTA PONENTE

La asambleísta ponente del presente proyecto de ley y del presente informe es la asambleísta Inés Margarita Alarcón Bueno, Presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral.

8. NOMBRE Y FIRMA DE LOS ASAMBLEÍSTAS QUE SUSCRIBEN EL INFORME

Inés Margarita Alarcón Bueno **Presidenta**	Firmado electrónicamente por: INES MARGARITA ALARCON BUENO Validar únicamente con FirmaEC
Andrés Felipe Castillo Maldonado **Vicepresidente**	Firmado electrónicamente por: ANDRES FELIPE CASTILLO MALDONADO Validar únicamente con FirmaEC
Camila Anahí Cueva Toro	Firmado electrónicamente por: CAMILA ANAHI CUEVA TORO Validar únicamente con FirmaEC
Mario Amado Zambrano Vera	Firmado electrónicamente por: MARIO AMADO ZAMBRANO VERA Validar únicamente con FirmaEC
Gema Karolina Dueñas Palma	Firmado electrónicamente por: GEMA KAROLINA DUENAS PALMA Validar únicamente con FirmaEC

Francisco Andrés Cevallos Macías	Firmado electrónicamente por: FRANCISCO ANDRES CEVALLOS MACIAS Validar únicamente con FirmaEC
Mariana Yumbay Yallico	
Gerardo Eugenio Machado Clavijo	
Jhajaira Estefanía Urresta Guzmán	Firmado electrónicamente por: JHAJAIRA ESTEFANIA URRESTA GUZMAN Validar únicamente con FirmaEC
Jahiren Elizabeth Noriega Donoso	

LAS SEÑORAS Y LOS SEÑORES ASAMBLEÍSTAS QUE SUSCRIBEN EL PRESENTE Informe para Segundo Debate del **"PROYECTO DE LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD"**

9. PROYECTO DE LEY DEBATIDO Y APROBADO.

EXPOSICIÓN DE MOTIVOS

La transformación digital del Estado ecuatoriano, impulsada por el desarrollo de tecnologías emergentes y la digitalización acelerada de servicios públicos y privados, ha generado nuevas oportunidades para la eficiencia institucional, la inclusión social, la innovación económica y el acceso ciudadano. No obstante, este proceso ha ampliado de manera significativa la superficie de exposición del país, generando escenarios de riesgo que comprometen a la administración pública, a la infraestructura crítica nacional y a millones de personas usuarias de servicios digitales. La consolidación de un Estado moderno exige que la digitalización vaya acompañada de mecanismos sólidos de seguridad, resiliencia y protección de activos estratégicos.

Sin embargo, esta misma transición ha expuesto a la administración pública, a la infraestructura crítica nacional, y a millones de personas usuarias a crecientes riesgos digitales: ciberataques, accesos indebidos, filtraciones de datos, interrupciones de servicios esenciales y vulnerabilidades estructurales que pueden comprometer la

estabilidad operativa del Estado. Estos riesgos no solo afectan a la prestación regular de servicios, sino que pueden generar impactos en la economía, la seguridad nacional y la confianza institucional.

En consonancia con la Política Pública para la Transformación Digital del Ecuador 2025-2030, que reconoce a la ciberseguridad como un eje esencial para generar confianza, proteger la información y asegurar la continuidad de los servicios digitales, esta propuesta legislativa incorpora de manera estructural el fortalecimiento de la seguridad digital como condición habilitante del proceso de transformación digital. Asimismo, se articula con la Política Nacional de Ciberseguridad, aprobada por el Gabinete Sectorial de Seguridad, y con la Estrategia Nacional de Ciberseguridad[25], instrumentos que establecen lineamientos técnicos para la protección de infraestructura crítica digital, la gestión de incidentes, la reducción de brechas de seguridad, la coordinación interinstitucional y la adopción de estándares internacionales. La presente reforma integra de forma normativa estos principios, orientaciones estratégicas y directrices operativas, asegurando que la gobernanza digital del país se fundamente en un ecosistema confiable, resiliente y alineado con las mejores prácticas internacionales.

Con el fin de garantizar la continuidad operativa del Estado y priorizar la protección de funciones esenciales, la presente reforma incorpora un instrumento técnico central: el Catálogo Nacional de Servicios Esenciales e Infraestructura Crítica Digital. Este catálogo permitirá identificar, clasificar y priorizar los servicios cuya interrupción tendría impactos severos en la vida, la salud, la economía, la seguridad pública y la estabilidad institucional, siguiendo criterios objetivos y estándares internacionales. Su incorporación normativa constituye un avance sustancial en la consolidación de una arquitectura de ciberseguridad basada en riesgo, y ordena las capacidades estatales según interdependencias sectoriales y niveles de criticidad.

Asimismo, dicha política establece como prioridad la protección de la infraestructura crítica digital, entendida como el conjunto de sistemas cuya alteración comprometería funciones esenciales del Estado o la sociedad. Esta ley incorpora esa visión estratégica mediante disposiciones que permiten identificar, clasificar y regular dicha infraestructura bajo principios de proporcionalidad, gestión de riesgos y continuidad operativa. La creación del Catálogo Nacional de Servicios Esenciales e Infraestructura Crítica Digital ofrece por primera vez un instrumento técnico, dinámico y basado en riesgo para ordenar y priorizar las capacidades de seguridad del país.

La acelerada evolución de tecnologías emergentes —particularmente la computación cuántica— introduce riesgos inéditos para los sistemas criptográficos que actualmente sustentan la confidencialidad, integridad y autenticidad de las comunicaciones electrónicas del Estado y del sector privado. Diversos organismos internacionales (NIST, ENISA, ETSI) han advertido que los algoritmos criptográficos tradicionales podrían volverse vulnerables frente a capacidades cuánticas, comprometiendo mecanismos esenciales como el cifrado de datos sensibles, la firma digital, la infraestructura de clave pública y los protocolos críticos utilizados para la continuidad operativa de servicios

[25] La articulación normativa señalada se sustenta en tres instrumentos rectores de la política pública nacional: (i) la Política Pública para la Transformación Digital del Ecuador 2025–2030, aprobada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información; (ii) la Política Nacional de Ciberseguridad, publicada mediante Acuerdo Ministerial Nro. 006-2021 de 17 de mayo de 2021; y (iii) la Estrategia Nacional de Ciberseguridad.

esenciales. En este contexto, la presente reforma incorpora el principio de adaptabilidad tecnológica, que obliga al Estado a anticipar y mitigar estos riesgos mediante la actualización progresiva y continua de mecanismos criptográficos, así como la adopción de estándares internacionales de protección frente a amenazas cuánticas. Esta orientación estratégica fortalece la resiliencia del ecosistema digital nacional y garantiza la sostenibilidad de la transformación digital a largo plazo.

El modelo de gobernanza promovido por la política también impulsa la articulación entre entidades públicas, sector privado, academia y sociedad civil, reconociendo que la ciberseguridad es un desafío compartido. La presente reforma asume esa visión mediante mecanismos de coordinación interinstitucional, cooperación internacional y procesos de consulta pública para la emisión de normativa secundaria. Asimismo, respeta las competencias de los órganos de regulación y control especializados, garantizando que la rectoría en ciberseguridad complemente, y no sustituya, la labor sectorial.

En este contexto, la ciberseguridad – entendida como el conjunto de políticas, prácticas, estándares y mecanismos orientados a proteger la confidencialidad, integridad y disponibilidad de los activos digitales – no puede ser tratada como un componente accesorio o paralelo al proceso de transformación digital. La ciberseguridad constituye un elemento estructural de la gobernanza digital y un prerrequisito para que la modernización administrativa sea sostenible, confiable y segura.

No puede hablarse de transformación digital efectiva si los sistemas que la sustentan son vulnerables, si los servicios que se ofrecen son fácilmente interrumpibles, o si los datos personales e institucionales están expuestos a ataques o mal uso. La confianza pública, la legitimidad institucional y la continuidad de los servicios esenciales dependen directamente de la existencia de un entorno digital seguro y resiliente. En otras palabras, no hay transformación digital sin ciberseguridad. La experiencia internacional ratifica este principio: los Estados que han integrado la ciberseguridad en su arquitectura de transformación digital han logrado reducir vulnerabilidades, fortalecer su capacidad de respuesta y consolidar marcos regulatorios coherentes con las necesidades del siglo XXI.

Este principio orientador es el que sustenta la decisión de reformar directamente la Ley Orgánica para la Transformación Digital y Audiovisual, y no crear un cuerpo normativo independiente. Optamos por esta vía para garantizar que el marco de transformación digital del Estado ecuatoriano incorpore, de manera estructural e inseparable, los principios, obligaciones y mecanismos de la ciberseguridad como parte integral de su gobernanza digital. No se trata de superponer una política sobre otra, sino de integrar la seguridad en el diseño mismo del ecosistema digital del país. La integración permite evitar duplicidad de marcos legales, asegurar coherencia institucional y fortalecer el rol del ente rector en transformación digital como articulador del sistema nacional de ciberseguridad.

La presente Ley tiene como objetivo fortalecer el marco legal de la ciberseguridad en el Ecuador, mediante la incorporación de disposiciones especializadas dentro de la Ley Orgánica para la Transformación Digital y Audiovisual, sin alterar su estructura ni su enfoque general. Entre los elementos fundamentales de esta reforma destacan la definición de principios rectores de ciberseguridad; la creación de un catálogo nacional de infraestructura crítica digital; la regulación de la gestión de incidentes y su notificación

obligatoria, incluyendo un plazo máximo de setenta y dos (72) horas para reportar incidentes relevantes, en coherencia con estándares internacionales; la habilitación jurídica de prácticas de hacking ético bajo condiciones de consentimiento, finalidad legítima y responsabilidad profesional; la delimitación de obligaciones específicas para el sector público y privado; la fiscalización técnica y la evaluación del cumplimiento de medidas de seguridad; la articulación institucional con órganos de defensa, inteligencia, justicia, educación y protección de datos personales; y las directrices de cooperación internacional para fortalecer la capacidad del país frente a amenazas transnacionales.

El proyecto introduce además estándares mínimos nacionales de ciberseguridad, establece mecanismos de coordinación con CSIRTs sectoriales y consolida el funcionamiento del CSIRT Nacional como instancia técnica especializada.

Este proyecto no crea nuevas entidades ni estructuras orgánicas adicionales, y sus disposiciones pueden ser implementadas en el marco de las competencias vigentes del Ministerio rector de transformación digital, en coordinación con las autoridades sectoriales. De esta manera, se cumple con el principio de sostenibilidad fiscal consagrado en el artículo 287 de la Constitución de la República del Ecuador. La reforma optimiza capacidades existentes y ordena funciones dispersas, evitando impactos presupuestarios y fortaleciendo la eficiencia administrativa.

Además, se ha garantizado la armonización normativa con la Ley Orgánica de Protección de Datos Personales (LOPDP), respetando la autonomía y competencia exclusiva de la autoridad de protección de datos. Las acciones propuestas se articulan técnicamente con dicha ley, asegurando la protección integral de los derechos digitales sin duplicidad funcional ni interferencia institucional. En este sentido, toda actuación que involucre tratamiento de datos personales deberá coordinarse con la autoridad especializada, garantizando un diseño regulatorio coherente y respetuoso de la privacidad.

En suma, esta propuesta normativa busca dotar al Estado ecuatoriano de una arquitectura moderna y eficaz que refuerce su capacidad para enfrentar amenazas cibernéticas, proteger activos digitales estratégicos y consolidar un ecosistema digital confiable, soberano y resiliente. Esta reforma posiciona a la ciberseguridad como columna vertebral del proceso de transformación digital, asegurando que este no sea solo un salto tecnológico, sino una verdadera evolución institucional con bases sólidas y seguras. Su implementación permitirá fortalecer la seguridad nacional, mejorar la prestación de servicios esenciales, incrementar la confianza ciudadana y proyectar al Ecuador hacia un modelo de gobernanza digital moderno y alineado con los estándares internacionales.

La oportunidad de esta reforma también se sustenta en el marco normativo vigente, particularmente en el Decreto Ejecutivo Nro. 464 de 22 de noviembre de 2024, mediante el cual el Presidente de la República creó el Comité Nacional de Ciberseguridad, definió su composición interinstitucional y le otorgó la facultad de aprobar la Política Nacional de Ciberseguridad y emitir directrices vinculantes. Esta decisión normativa refuerza el principio de rectoría pública, consolida el papel del Ministerio de Telecomunicaciones y de la Sociedad de la Información como ente rector, y constituye un precedente ejecutivo fundamental que habilita la presente reforma legal. La presente ley incorpora de manera estable y vinculante el modelo institucional de dicho decreto, garantizando continuidad, seguridad jurídica y coherencia estratégica en la gestión nacional de la ciberseguridad.

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-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).

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 obligatorio 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-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 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 ataque 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.- 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 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.

Artículo 20-T.- Sanciones por infracciones graves.- El ente rector de ciberseguridad impondrán 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.

Artículo 20-U.- Infracciones muy graves.- El ente rector de ciberseguridad impondrán 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

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 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.

Artículo 20-Y.- Coordinación interinstitucional y no 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 fijo y móvil de órbita baja (LEO) que operen a través de Estaciones Terrenas en Movimiento (ESIM), seguirá 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."

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 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.

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 CSIRTs 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 CSIRTs 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 reformatoria entrará en vigencia a partir de su publicación en el Registro Oficial.

10. CERTIFICACIÓN:

En mi calidad de Secretario Relator de la Comisión Especializada de la COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN Y SEGURIDAD INTEGRAL

CERTIFICO:

Que, el presente Informe para Segundo Debate del **"PROYECTO DE LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD"**, fue conocido, debatido y aprobado en la Sesión **Nro. 061** del 30 de enero de 2026, en el Pleno de la COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN Y SEGURIDAD INTEGRAL, con la siguiente votación: AFIRMATIVO: SIETE (7). NEGATIVO: CERO (0) ABSTENCIÓN: TRES (3). ASAMBLEÍSTAS AUSENTES: (CERO).

Quito D.M., 30 de enero del 2026

Atentamente,

Firmado electrónicamente por:
MARCO DANILO JIRON PAREDES
Validar únicamente con FirmaEC

Mgt. Marco Jirón
SECRETARIO RELATOR DE LA COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN Y SEGURIDAD INTEGRAL