2025-10-31

Señora Presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral,
Señoras y Señores Asambleístas de la Comisión:

En el presente documento expongo mi perspectiva, observaciones y recomendaciones sobre el Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, Reformatoria a la Ley Orgánica de Transformación Digital y Audiovisual, basadas en mi experiencia en los campos de la ciberseguridad, la ingeniería de software y arquitectura, y la ingeniería de sistemas.

Quisiera comenzar aclarando que el proyecto de ley actual contiene numerosos aspectos positivos. Es urgente que el Ecuador cuente con una ley integral de ciberseguridad que contribuya a reducir el número de vulnerabilidades y ataques que actualmente afectan al país. Este proyecto constituye un paso en la dirección correcta; sin embargo, también representa una oportunidad valiosa para fortalecer varios aspectos que aún presentan deficiencias.

Mi perspectiva sobre las necesidades del Ecuador se fundamenta en un concepto que denomino Soberanía Digital. Considero crucial que el país fortalezca su infraestructura local, pero también la disponibilidad de servicios locales. En la actualidad, muchos servicios públicos dependen de empresas estadounidenses. Un ejemplo de ello es que tanto la Asamblea Nacional como el Consejo de la Judicatura utilizan Facebook para transmitir audiencias de interés público. ¿Qué ocurriría si una de esas audiencias contuviera información desfavorable para Facebook o Meta? Existe un riesgo real de que las cuentas o páginas utilizadas para dichas transmisiones puedan ser canceladas o bloqueadas.

¿Debería realmente ser posible que una empresa privada extranjera determine lo que el público ecuatoriano puede o no puede ver? Otro aspecto problemático de este tipo de dependencia es que la información privada de las y los ecuatorianos es recopilada por Facebook cuando desean acceder a transmisiones de interés público.
Mi recomendación general es que el Ecuador procure depender menos de proveedores internacionales como Google, Starlink y Facebook, y que, en su lugar, fomente un mayor desarrollo local. Esto permitirá crear más conocimiento y productos nacionales, impulsando un mercado interno más productivo, al tiempo que se fortalecen las capacidades locales de ciberseguridad, las cuales, en última instancia, contribuirán a la protección del país.

En general, todas las recomendaciones de este documento están guiadas por esta perspectiva.

También es importante mencionar que la seguridad nunca será perfecta; esta es una característica inherente a su propia naturaleza. En términos generales, se aplican medidas para protegerse frente a ciertos riesgos. Dichas medidas tienen un costo, y por esa razón no es racional aplicar todas las medidas posibles frente a todos los riesgos posibles, pues ello implicaría un costo infinito. En su lugar, se deben tomar decisiones racionales sobre qué riesgos se desea mitigar y de qué manera.

Dicho esto, existen otras medidas que tienen un impacto muy negativo sobre la seguridad. En el contexto de este documento, me refiero principalmente a la censura y a la inclusión de puertas traseras (backdoors). Un experto previo ante esta Comisión mencionó el Gran Cortafuegos de China como un ejemplo que Ecuador debería emular para proteger a la población. Sin embargo, tal enfoque solo serviría para censurar, debilitando de manera significativa la ciberseguridad nacional. Recomiendo enfáticamente no seguir ese camino: debemos fortalecer la ciberseguridad, no debilitarla.

Además, cabe destacar que la mayoría de las plataformas ya disponen de mecanismos para proteger a los segmentos más vulnerables de la población, como niñas, niños y adolescentes. Sistemas como Android, iPhone y Windows incluyen controles parentales sin costo adicional.

Recomendación: Cédula Digital

Para apoyar una autenticación más segura en los servicios públicos, recomiendo la implementación de una cédula digital que pueda utilizarse para la identificación en cualquier interacción con servicios públicos y, potencialmente, también en servicios privados.

Esto permitiría implementar sistemas de autenticación más avanzados, como autenticación multifactor, autenticación basada en tokens u otras variantes.

Actualmente, los sistemas utilizados en el sector público no cuentan con un esquema común de nombres de usuario y contraseñas, lo que ha llevado a la proliferación de múltiples credenciales en diferentes sistemas —como el SRI o Quipux— y a niveles de seguridad variables, ya que cada sistema aplica protecciones diferentes.

El uso de un sistema de identidad digital puede implementarse de diversas maneras. Suecia utiliza un sistema denominado BankID, donde los bancos son responsables de la identificación de los individuos. Estonia e India cuentan con sistemas gestionados por el gobierno central. La misma infraestructura utilizada actualmente para la firma digital podría ampliarse para soportar un sistema nacional de identidad digital.

Recomendación: Autenticación Multifactor en Todos los Sistemas Públicos

Relacionado con la recomendación anterior, propongo establecer la obligatoriedad de autenticación multifactor en todos los sistemas públicos.

Dado que las contraseñas suelen ser débiles y susceptibles a distintos tipos de robo, las recomendaciones internacionales actuales señalan que siempre se debe emplear más de un factor de autenticación.

Considero importante que esta obligación sea legislada para reforzar la seguridad de todos los sistemas gubernamentales.

Si bien esta medida podría implementarse de forma independiente al proyecto de cédula digital, hacerlo así implicaría una duplicación considerable de esfuerzos.

Recomendación: Preferir Software Libre y de Código Abierto

Varias partes del proyecto de ley mencionan el principio de neutralidad tecnológica, lo cual constituye un ideal loable. Sin embargo, desde el punto de vista de la ciberseguridad, este principio no siempre conduce a las mejores decisiones.

Mi recomendación es dar preferencia al software libre y de código abierto, aquel cuyo código fuente puede ser leído y mejorado por cualquier persona.

En general, este tipo de software tiende a ser más seguro y, además, permite que ingenieras e ingenieros locales contribuyan, ofrezcan soporte e incluso generen emprendimientos basados en dicha colaboración, fortaleciendo así la soberanía digital del país.

Recomendación: Implementar “Safe Harbor” y Protecciones Similares para Investigadores

El Ecuador es uno de los países que cuenta con pocos investigadores en ciberseguridad que publiquen sus hallazgos.

Una de las razones es la incertidumbre legal existente respecto a este tipo de trabajo.

En muchos otros países, las y los investigadores independientes descubren vulnerabilidades y las reportan a las entidades correspondientes; sin embargo, esto casi nunca ocurre en Ecuador debido al riesgo de ser procesados penalmente.

Mi recomendación es implementar leyes de “puerto seguro” (safe harbor) que protejan a los investigadores en ciberseguridad que actúan de buena fe.

Este tipo de protección existe o se encuentra en discusión en varios países, incluyendo la Unión Europea, Alemania y Australia.

En los Estados Unidos, el Departamento de Justicia ha emitido una política que establece que no perseguirá judicialmente a los investigadores que trabajen de buena fe.

Recomendación: Políticas para la Recepción de Reportes de Seguridad

De manera complementaria, es necesario que los investigadores puedan reportar vulnerabilidades de forma segura a las instituciones correspondientes.

Para que este proceso funcione, deben existir políticas claras sobre cómo se gestionarán estos reportes.

El primer paso básico es definir una dirección o canal oficial para recibirlos.

Asimismo, es indispensable incluir medidas de seguridad como el uso de correo electrónico cifrado, a fin de proteger la información sensible que pueda ser enviada.

Recomiendo que todas las instituciones públicas estén obligadas a publicar una política de seguridad que contemple estos mecanismos.

Recomendación: Actualizar la Firma Digital con Criptografía Post-Cuántica Moderna

El sistema de firma digital utilizado actualmente en Ecuador emplea algoritmos antiguos que quedarán obsoletos en pocos años debido al avance de los computadores cuánticos.

Cuando estos alcancen suficiente capacidad, será posible falsificar las firmas actuales, lo que haría perder toda la confianza existente en el sistema.

Antes de que esto ocurra, es urgente actualizar los algoritmos a variantes post-cuánticas, capaces de resistir ataques provenientes de la computación cuántica.

Dado que implementar este cambio llevará tiempo, recomiendo legislar su adopción de manera inmediata, a fin de iniciar el trabajo técnico necesario con la debida anticipación.

Recomendación: Requerir un Informe Post-Mortem para Todos los Incidentes Reportados

El proyecto de ley actual establece, en varios apartados, la obligación de reportar incidentes de ciberseguridad.

Aunque esto representa un avance importante, sería extremadamente útil requerir un informe post-mortem posterior a cada incidente.

Este documento debe describir lo que funcionó bien, lo que falló y las medidas que se adoptarán para mejorar la preparación ante futuros incidentes.

Dichos informes serían valiosos para el Estado, ya que permitirían recopilar no solo estadísticas, sino también información cualitativa sobre los tipos de amenazas que enfrenta el Ecuador y las respuestas aplicadas.

Recomendación: Fomentar la Educación en Ciberseguridad

Recomiendo enfatizar la necesidad de fortalecer la formación en ciberseguridad en el Ecuador.

Esto podría lograrse mediante la creación de un Plan Nacional de Formación en Ciberseguridad, que garantice la preparación de una nueva generación de profesionales capaces de proteger al país frente a los desafíos tecnológicos actuales y futuros.

Recomendación: Fortalecer la Colaboración con el Sector Privado y la Academia

Para asegurar un marco nacional de ciberseguridad sólido y adaptable, el Ecuador debe promover formalmente la participación del sector privado y la academia en el diseño e implementación de políticas de ciberseguridad.

El sector privado gestiona buena parte de la infraestructura digital crítica del país y posee experiencia directa en la detección de amenazas y vulnerabilidades, mientras que la academia aporta la capacidad de investigación y la formación técnica necesarias para construir experiencia nacional sostenible.

El establecimiento de mecanismos estructurados de colaboración —como consejos consultivos, programas de investigación conjunta e iniciativas de respuesta coordinada a incidentes— permitiría al Ecuador beneficiarse de perspectivas diversas, acelerar la innovación y fortalecer su capacidad de respuesta ante amenazas emergentes.

La inclusión de estos sectores en la gobernanza nacional de la ciberseguridad aumentará la resiliencia técnica, la transparencia y la madurez del ecosistema digital ecuatoriano.

Recomendación: Prohibición de Puertas Traseras (Backdoors) en los Sistemas Nacionales

Para salvaguardar la soberanía digital, la privacidad y la resiliencia del Ecuador, es esencial que la legislación nacional prohíba explícitamente la inclusión de cualquier tipo de puerta trasera o mecanismo de acceso oculto en sistemas informáticos, software o infraestructura de telecomunicaciones desplegada en el país.

Estos mecanismos —ya sean intencionales o impuestos— socavan la confianza pública, debilitan la seguridad nacional y crean vulnerabilidades sistémicas que pueden ser explotadas por actores maliciosos.

Garantizar que los sistemas estén libres de accesos ocultos es fundamental para proteger los derechos de la ciudadanía, la confidencialidad de la información estatal y privada, y la integridad de la infraestructura digital crítica del Ecuador.

La legislación debe establecer mecanismos de responsabilidad y sanción frente a la creación, implementación o exigencia de este tipo de accesos, además de promover el uso de estándares abiertos, auditorías de código independientes y revisiones de seguridad transparentes.

De esta manera, el Ecuador podrá consolidarse como líder regional en ciberseguridad y en la protección de los derechos digitales.

Recomendación: Creación de un Registro Central de Incidentes de Ciberseguridad

El Ecuador debería crear un registro nacional de incidentes de ciberseguridad, que funcione como un mecanismo centralizado para recopilar, analizar y compartir información sobre los eventos de seguridad que afecten tanto a entidades públicas como privadas.

Un registro coordinado fortalecería la conciencia situacional, permitiría identificar riesgos sistémicos con mayor rapidez y apoyaría la toma de decisiones basadas en evidencia.

El registro debe operar bajo estrictas normas de confidencialidad y protección de datos, garantizando que la información sensible reportada por las organizaciones permanezca protegida.

La participación debería ser obligatoria para los operadores de infraestructura crítica y voluntaria con incentivos para otros sectores.

Con esta medida, el Ecuador podría mejorar su resiliencia nacional, promover la transparencia y desarrollar una visión integral de su panorama de ciberseguridad.

Recomendación: Implementar un Marco Nacional de Clasificación de Riesgos Cibernéticos

El Ecuador debería desarrollar e implementar un marco nacional para la clasificación de riesgos cibernéticos, que estandarice la forma en que se evalúan y priorizan las amenazas, vulnerabilidades e incidentes en los distintos sectores.

Un marco unificado permitiría aplicar metodologías coherentes para evaluar el impacto y la probabilidad de los riesgos, facilitando una mejor asignación de recursos y una coordinación más efectiva de la defensa nacional.

Este marco debería alinearse con estándares internacionales (como ISO 27005, NIST SP 800-30 o las guías de ENISA), adaptándose al contexto regulatorio, económico y tecnológico del Ecuador.

Adoptar un lenguaje común para la evaluación de riesgos fortalecerá la coordinación entre actores públicos y privados, mejorará la toma de decisiones y aumentará la resiliencia del ecosistema digital nacional.

Recomendación: Implementar un Programa Voluntario de Certificación en Ciberseguridad para el Sector Privado

El Ecuador debería establecer un programa nacional de certificación voluntaria en ciberseguridad para las organizaciones del sector privado, con el objetivo de elevar los estándares de seguridad y fomentar una cultura de mejora continua.

Este programa permitiría a las empresas demostrar su compromiso con las mejores prácticas internacionales en ciberseguridad, fortaleciendo la confianza de clientes, socios y reguladores.

El proceso de certificación debería alinearse con marcos internacionales como ISO/IEC 27001, NIST CSF o los Controles CIS, y adaptarse a las capacidades de organizaciones de distintos tamaños.

Incentivos como reconocimiento público, ventajas en contratación pública o acceso a programas estatales de apoyo podrían fomentar la participación voluntaria.

De esta manera, el Ecuador impulsaría la inversión en ciberseguridad, elevaría los estándares nacionales y consolidaría la cooperación público-privada para proteger la infraestructura digital del país.

Propuestas de Cambio al Artículo 20

Literales a) y b): El texto actual utiliza los términos “garantizar” para “Confidencialidad” y “asegurar” para “Integridad”. Técnicamente, esto no es posible, ya que la seguridad nunca es absoluta. Recomiendo modificar el lenguaje para evitar expresiones que impliquen una garantía total.

Inclusión de nuevos conceptos: Sugiero incorporar las propiedades de “Autenticidad” y “Trazabilidad” como componentes esenciales de un sistema seguro.

Literal f): En concordancia con la recomendación sobre software libre, recomiendo que se incorpore una preferencia por el software libre y de código abierto.

Propuesta de Cambio al Artículo 20-B y 20-G

En relación con la recomendación sobre los informes post-mortem, propongo que se añada la obligación de presentar un informe post-mortem una vez resuelto cada incidente, describiendo las lecciones aprendidas y las medidas correctivas implementadas.

Conclusión

El Ecuador se encuentra en un momento decisivo de su transformación digital. El proyecto de ley de ciberseguridad representa una oportunidad crítica para sentar las

bases de un futuro digital más seguro, resiliente y soberano. Sin embargo, la verdadera ciberseguridad no puede alcanzarse mediante medidas aisladas; requiere una estrategia nacional coherente, inclusiva y con visión de futuro.

Las recomendaciones presentadas en este documento buscan fortalecer el proyecto de ley, resaltando los principios de transparencia, colaboración, independencia tecnológica y aprendizaje continuo.

La construcción de un ecosistema digital seguro requiere confianza: confianza en la integridad de los sistemas, en la protección de los derechos ciudadanos y en las instituciones responsables de garantizarla.

Esa confianza solo será posible si el Ecuador prioriza la apertura, la rendición de cuentas y la participación activa del sector privado, la academia y la sociedad civil.

Al adoptar políticas que promuevan la soberanía digital, prohíban las puertas traseras, protejan a los investigadores, fomenten la educación y alineen las prácticas nacionales con los estándares internacionales, el Ecuador no solo fortalecerá su postura en materia de ciberseguridad, sino que también podrá consolidarse como un referente regional en la defensa de la privacidad, la innovación y los derechos humanos en la era digital.

Finalmente, deseo expresar mi más sincero agradecimiento a las y los miembros de la Asamblea Nacional y de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral por haberme invitado y permitido contribuir en este importante proceso legislativo.

Es un honor poder apoyar los esfuerzos del Ecuador para construir un futuro digital más seguro, soberano y resiliente.

Atentamente,

Ola Metodius Martin Bini
Time Stamping Security Data

Ola Bini
Director Técnico
Seguridad Digital EC
CI: 1760044600
ola@seguridaddigital.ec