ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR
DEL DIÁLOGO
¡A los hechos!

Memorando Nro. AN-CSIS-2023-0123-M

Quito, D.M., 23 de marzo de 2023

PARA: Sr. Dr. Javier Virgilio Saquicela Espinoza
Presidente de la Asamblea Nacional

ASUNTO: Envío Informe para Primer Debate Ley Orgánica de Seguridad Digital

De mi consideración:

Reciba un cordial saludo, por disposición del Presidente de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, Asambleísta Ramiro Narváez Garzón, adjunto el **Informe para primer debate del proyecto de Ley Orgánica de Seguridad Digital,** aprobado en la sesión 219 realizada el día miércoles 22 de marzo de 2023.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Abg. Javier Andres Borja Ortiz
SECRETARIO RELATOR

Anexos:
- 22.03.2023_cepsisi_informe_primer_debate-signed_vf.pdf

Copia:
Sr. Ramiro Vladimir Narváez Garzón
Presidente de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral

Sr. Abg. Galo Fernando Terán Varela
Prosecretario Relator

Sra. Maria Fernanda Bermudez Rodriguez
Asistente de Asambleísta

Firmado electrónicamente por:
JAVIER ANDRES BORJA ORTIZ

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR
LEGISLAMOS PARA LA VIDA

COMISIÓN DE SOBERANÍA, INTEGRACIÓN Y SEGURIDAD INTEGRAL

Comisión No. 13

INFORME PARA PRIMER DEBATE

PROYECTO DE LEY ORGÁNICA DE SEGURIDAD DIGITAL

Integrantes

- Ramiro Vladimir Narváez Garzón, presidente
- Patricia Núñez Ramos, vicepresidenta
- Rodrigo Olmedo Fajardo Campoverde
- Augusto Alejandro Guamán Rivera
- Xavier Andrés Jurado Bedrán
- Jorge Washington Pinto Dávila
- Simón Bolívar Remache
- José Luis Vallejo Ayala
- Geraldine Weber Moreno

22 de marzo de 2023

Quito D.M., Ecuador

CONTENIDO

TABLAS:

INFORME PARA PRIMER DEBATE

LEY ORGÁNICA DE SEGURIDAD DIGITAL

1. OBJETO DEL INFORME

El presente informe tiene como objeto poner en conocimiento del Pleno de la Asamblea Nacional el texto del Proyecto de Ley Orgánica de Seguridad Digital, que unifica tres iniciativas que han sido procesadas para su tratamiento por parte de la Comisión de Soberanía, Integración y Seguridad Integral, en 17 sesiones ordinarias en las que se acogió y procesó las observaciones y aportes de las instituciones, expertos y representantes de los profesionales de la seguridad digital.

Expone, en síntesis, el debate que ha realizado la Comisión respecto a la regulación del Sistema Nacional de Seguridad Digital y sus subsistemas de ciberdefensa, ciberinteligencia, ciberdiplomacia y ciberseguridad ciudadana.

El proyecto propone aportar al fortalecimiento de la ciberseguridad de conformidad con los más altos estándares internacionales, a fin de permitir que el país se convierta en un referente regional y mundial en materia de seguridad digital y de la información.

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-SG-2021-1763-M de 15 de junio de 2021, el abogado Álvaro Salazar Paredes, Secretario General de la Asamblea Nacional, notificó la Resolución CAL-2021-2023-010 de fecha 14 de junio de 2021, en la que el Consejo de Administración Legislativa decidió aprobar la distribución de proyectos de ley y de instrumentos internacionales tanto para la Comisión de Soberanía, Integración y Seguridad Integral, como para la Comisión de Relaciones Internacionales y Movilidad Humana, conforme el detalle constante en el Anexo Único.

- En Sesión Ordinaria Nro. 003 realizada el 11 de junio de 2021, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral aprobó su Plan de Trabajo para el período junio 2021 – mayo 2023 mediante el cual, en su punto 4.1., priorizó el tratamiento del proyecto de Ley de Seguridad Digital presentado por el asambleísta Juan Carlos Yar.

- En Sesión Ordinaria Nro. 005 realizada el 23 de junio de 2021, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral trató como tercer punto del orden del día el siguiente: "*Conocimiento debate y votación del Proyecto de Resolución PROYECTO DE RESOLUCIÓN QUE EXPRESA EL COMPROMISO DE LA COMISIÓN CON LA SEGURIDAD INTEGRAL Y EXHORTA AL PRESIDENTE DE LA REPÚBLICA DEL ECUADOR SE HAGAN LOS ESFUERZOS NECESARIOS PARA SUSCRIBIR EL CONVENIO DE BUDAPEST SOBRE CIBERDELINCUENCIA",* presentado por el Asambleísta Rodrigo Fajardo y aprobó la mencionada resolución.

- En Sesión Ordinaria Nro. 020 realizada el 06 de agosto de 2021, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral conoció el "Proyecto de Ley de Seguridad Digital", presentado por el ex asambleísta Juan Carlos Yar y, en la misma sesión, aprobó la moción para su unificación a Código Orgánica de Seguridad Integral.

- En Sesión Ordinaria Nro. 31 realizada el 27 de agosto de 2021, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibió al experto Daniel Tenorio para que presente sus observaciones al texto del proyecto de Ley de Seguridad Digital y la parte correspondiente a ciberseguridad del proyecto de Código Orgánico de Seguridad del Estado.

- En Sesión Ordinaria Nro. 38 realizada el viernes 17 de septiembre de 2021, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibió al Señor ingeniero Gabriel Llumiquinga y doctor Santiago Acurio, presidente y vicepresidente, respectivamente, de la Asociación Ecuatoriana de Ciberseguridad, para que presente sus observaciones al texto del proyecto de Ley de Seguridad Digital y la parte correspondiente a ciberseguridad del proyecto de Código Orgánico de Seguridad del Estado.

- Mediante Memorando Nro. AN-SG-2021-3873-M de 21 de noviembre de 2021, el abogado Álvaro Salazar Paredes, Secretario General de la Asamblea Nacional, notificó al Presidente de la Comisión de Soberanía, Integración y Seguridad Integral con la Resolución CAL-2021-2023-195 de fecha 18 de noviembre de 2021, en la que el Consejo de Administración Legislativa decidió calificar el "Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia", presentado por el asambleísta Rodrigo Fajardo Campoverde, mediante Memorando Nro. AN-FCRO-2021-0063-M de 19 de octubre de 2021.

- En Sesión Ordinaria Nro. 059 realizada el 24 de noviembre de 2021, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral avocó conocimiento del "Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia", presentado por el asambleísta Rodrigo Fajardo Campoverde y escuchó sus motivaciones para la presentación del mismo y, en la misma sesión aprobó la moción para su unificación a Código Orgánica de Seguridad Integral.

- En la Sesión Ordinaria Nro. 064 realizada el 3 de diciembre de 2021 la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibió al doctor Alejandro Padín Vidal experto español en materia de Ciberseguridad, para que brinde sus observaciones y

recomendaciones al proyecto de Código Orgánico de Seguridad del Estado, en la parte correspondiente a ciberseguridad.

- Mediante Memorando Nro. AN-SG-2022-0777-M de 04 de marzo de 2022, el abogado Álvaro Salazar Paredes, Secretario General de la Asamblea Nacional, notificó al Presidente de la Comisión de Soberanía, Integración y Seguridad Integral con la Resolución CAL-2021-2023-403 de fecha 28 de febrero de 2022, en la que el Consejo de Administración Legislativa decidió calificar el "Proyecto de Ley Orgánica de Ciber Seguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos" presentado por el asambleísta José Luis Vallejo Ayala; mediante Oficio No. AN-VAJL-2021-0047-O de 14 de diciembre de 2021.

- En Sesión Nro. 098 realizada el 08 de marzo de 2022, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral avocó conocimiento del "Proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos", presentado por el señor asambleísta José Luis Vallejo Ayala.

- En Sesión Ordinaria 107 de 30 de marzo de 2022, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral conoció las motivaciones y argumentaciones del "Proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos", a cargo del señor asambleísta José Luis Vallejo Ayala, PhD.

- En Sesión Ordinaria 109 de 06 de abril de 2022, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral conoció y resolvió sobre la propuesta de unificación del Proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos al Proyecto de Código Orgánico de Seguridad Integral, mediante moción del Asambleísta Ramiro Narváez Garzón, acogida por unanimidad.

- El Presidente de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral solicitó aportes y observaciones los Proyectos de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia, Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos y Ley de Seguridad Digital a las siguientes autoridades:

  - Mediante Oficio Nro. AN-CSIS-2022-0311-O de 9 de junio de 2022, al Señor Cornel (SP) Fausto Antonio Cobo Montalvo, Director General del Centro de Inteligencia Estratégica.
  - Mediante Oficio Nro. AN-CSIS-2022-0312-O de 9 de junio de 2022, al Señor General (SP) Luis Eduardo Lara Jaramillo, Ministro de Defensa Nacional.
  - Mediante Oficio Nro. AN-CSIS-2022-0313-O de 9 de junio de 2022, al Señor General Inspector, Hernán Patricio Carrillo Rosero, entonces Ministro del Interior.
  - Mediante Oficio Nro. AN-CSIS-2022-0314-O de 09 de junio de 2022, a la Señor Vianna Di Maria Maino Isaias, Ministra de Telecomunicaciones y Sociedad de la Información.
  - Mediante Oficio Nro. AN-CSIS-2022-0315-O de 10 de junio de 2022, al Señor Magíster, Juan Carlos Holguín Maldonado, Ministro de Relaciones Exteriores y Movilidad Humana.

- En Sesión Ordinaria 132 de 15 de junio de 2022, la Comisión Especializada Permanente de Soberanía, Integración recibió a los delegados del Ministerio de Defensa Nacional, Ministerio de Relaciones Exteriores y Movilidad Humana, Ministerio del Interior, Centro de Inteligencia Estratégica; y, Ministerio de Telecomunicaciones y Sociedad de la Información, para que presenten sus observaciones en el marco del tratamiento de los proyectos de ciberseguridad.

- En Sesión Ordinaria 133 de 15 de junio de 2022, la Comisión Especializada Permanente de Soberanía, Integración recibió a la abogada María Alexandra Maldonado Navarro, magíster en Derecho Público y experta en seguridad digital; y, al Señor abogado Luis Fernando Enríquez Álvarez, Master of Laws y magíster en Derecho Mención Derecho Internacional Económico, miembro del Observatorio de Ciberderechos de la Universidad Andina Simón Bolívar, para que presenten sus observaciones en el marco del tratamiento de los proyectos de ciberseguridad.

- Mediante Oficio Nro. AN-CSIS-2022-0455-O de 17 de agosto de 2022, el Presidente de la Comisión de Soberanía, Integración y Seguridad Integral solicitó a la Ministra de Telecomunicaciones y Sociedad de la Información la designación de "*un equipo técnico o delegado del Ministerio que se convierta en la contratarte técnica de la Comisión en la elaboración del texto para primer debate de la normativa legal, proporcionado información y absolviendo inquietudes dada la amplia, profunda y altamente técnica temática".*

- Mediante Oficio Nro. AN-CSIS-2022-0456-O de 17 de agosto de 2022, el Presidente de la Comisión de Soberanía, Integración y Seguridad Integral solicitó al Ministro de Relaciones Exteriores y Movilidad Humana la designación de un "*equipo técnico o delegado del Ministerio que participe como contraparte técnica durante el proceso de elaboración del texto para primer debate de la normativa legal, proporcionado información respecto a los instrumentos internacionales; así como, con acciones de coordinación con organismos públicos y otras organizaciones internacionales que prestan asistencia técnica respecto a dicha temática.".*

- Mediante Memorando Nro. AN-CSIS-2022-0511-M de 19 de agosto de 2022, el Presidente de la Comisión de Soberanía, Integración y Seguridad Integral solicitó Coordinador General de Relaciones Internacionales "*interponga los oficios pertinentes y se realice las acciones institucionales e interagenciales que correspondan para solicitar a la Secretaría Interamericana del Comité Contra el Terrorismo, CICTE, de la Organización de Estados Americanos, presten su asistencia técnica a esta Comisión durante el trámite legislativo de aprobación del Proyecto de Ley".*

- En Sesión Ordinaria 157 de 24 de agosto de 2022 la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibió al señor abogado Diego Álvarez, asesor en materia de política pública Amazon Web Services AWS para que, en el marco de las iniciativas legislativas sobre ciberseguridad que se tramitan en la Comisión, realice sus sugerencias con miras a buscar la transformación digital del país y la protección de la información en el ciberespacio.

- En Sesión Ordinaria 160 de 31 de agosto de 2022 la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibió a Humberto Arthos delegado de la Agencia

de Regulación y Control de las Telecomunicaciones ARCOTEL, con la finalidad de recibir sus observaciones y recomendaciones los proyectos de ley sobre ciberseguridad.

- En Sesión Ordinaria 162 de 7 de septiembre de 2022 la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibió al Magíster Jonathan Marcelo Ramos Mera, Catedrático de Derechos Penal de la Universidad Central del Ecuador y Representante de la Asociación Académica Ecuatoriana de Derecho e Informática para que exponga sus observaciones y análisis a los proyectos de ciberseguridad.

- En Sesión Ordinaria 164 de 9 de septiembre de 2022 la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibió al Coronel en servicio pasivo Marcelo Gómez, delegado del Centro de Inteligencia Estratégica para que exponga sus observaciones y criterios a los proyectos de ciberseguridad.

- El Presidente de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, invitó a los delegados de varias instituciones públicas a participar en varias Mesas Técnicas para la revisión del Borrador Unificado de Proyecto de Ley Orgánica de Seguridad Digital:

  - Mediante Oficio Nro. AN-CSIS-2023-0042-O de 19 de enero de 2023, al Coronel (SP) Fausto Antonio Cobo Montalvo, Director del Centro de Inteligencia Estratégica; a reunión técnica de 20 de enero de 2023.
  - Mediante Oficio Nro. AN-CSIS-2023-0043-O de 19 de enero de 2023, al Señor General de División (SP) Luis Eduardo Lara Jaramillo, Ministro de Defensa Nacional; a reunión técnica de 20 de enero de 2023.
  - Mediante Oficio Nro. AN-CSIS-2023-0044-O de 19 de enero de 2023, al Señor Magister Juan Carlos Holguín Maldonado, Ministro de Relaciones Exteriores y Movilidad Humana; a reunión técnica de 20 de enero de 2023.
  - Mediante Oficio Nro. AN-CSIS-2023-0045-O de 19 de enero de 2023, al Señor Ingeniero Juan Ernesto Zapata Silva, Ministro del Interior; a reunión técnica de 20 de enero de 2023.
  - Mediante Oficio Nro. AN-CSIS-2023-0046-O de 19 de enero de 2023, a la Señora Vianna Di Maria Maino Isaias, Ministra de Telecomunicación y de la Sociedad de la Información; a reunión técnica de 20 de enero de 2023.
  - Mediante Oficio Nro. AN-CSIS-2023-0049-O de 20 de enero de 2023, invitó a participar a los delegados del Ministerio de Defensa Nacional, Ministerio del Interior, Centro de Inteligencia Estratégica, Ministerio de Relaciones Exteriores y Movilidad Humana, Ministerio de Telecomunicaciones y Sociedad de la Información, a la reunión técnica de 24 de enero de 2023.
  - Mediante Oficio Nro. AN-CSIS-2023-0050-O de 20 de enero de 2023, invitó a participar a Señor General, Fausto Lenin Salinas Samaniego, Comandante General de la Policía Nacional del Ecuador, a la reunión técnica de 24 de enero de 2023.

- Mediante Oficio Nro. AN-CSIS-2023-0061-O de 25 de enero de 2023, invitó a participar a los delegados del Ministerio de Defensa Nacional, Ministerio del Interior, Ministerio de Relaciones Exteriores y Movilidad Humana, Ministerio de Telecomunicaciones y Sociedad de la Información, Comandancia Nacional de Policía y Secretaría Nacional de Seguridad Pública y del Estado, a la reunión técnica de 27 de enero de 2023.
- Mediante Oficio Nro. AN-CSIS-2023-0063-O de 27 de enero de 2023, invitó a participar a los delegados del Centro de Inteligencia Estratégica, a reunión técnica de 27 de enero de 2023.
- Mediante Oficio Nro. AN-CSIS-2023-0068-O de 29 de enero de 2023, invitó a participar a los delegados del Ministerio de Defensa Nacional, Ministerio del Interior, Ministerio de Relaciones Exteriores y Movilidad Humana, Ministerio de Telecomunicaciones y Sociedad de la Información, Comandancia Nacional de Policía, Secretaría Nacional de Seguridad Pública y del Estado y Centro de Inteligencia Estratégica a la reunión técnica de 31 de enero y jueves 2 de febrero de 2023.

- Mediante Oficio Nro. AN-CSIS-2023-0085-O de 7 de febrero de 2023, la Vicepresidenta encargada de la Presidencia de la Comisión de Soberanía, Integración y Seguridad Integral, Asambleísta Patricia Núñez, invitó a participar a los delegados del Ministerio de Defensa Nacional, Ministerio del Interior, Ministerio de Relaciones Exteriores y Movilidad Humana, Ministerio de Telecomunicaciones y Sociedad de la Información y Secretaría Nacional de Seguridad Pública y del Estado, a la reunión técnica de 09 de febrero de 2023.

- Mediante Memorando Memorando Nro. AN-CSIS-2023-0059-M de 20 de febrero de 2023, la Vicepresidenta encarga de la Presidencia de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral de la Asamblea Nacional, asambleísta Patricia Núñez, remite a las y los legisladores de la Comisión, el borrador de "Proyecto de Ley Orgánica de Seguridad Digital".

- En la sesión Nro. 209 y 211 realizadas el 23 y 24 de febrero de 2023, respectivamente, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral analizó y debatió los textos del Proyecto de Ley Orgánica de Seguridad Digital.

- En Sesión Nro. 219 de fecha 22 de marzo de 2023, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral de la Asamblea Nacional, conoció, debatió y aprobó el "Informe para Primer Debate del Proyecto de Ley Orgánica de Seguridad Digital" con 8 votos de 8 asambleístas presentes.

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

2.2.1. Observaciones institucionales y ciudadanas recibidas en comisión general

En la siguiente tabla, se resumen las principales observaciones presentadas por los distintos actores institucionales, académicos y ciudadanos:

Tabla 1: Observaciones recibidas en comisión general

OBSERVACIONES RECIBIDAS EN COMISIÓN GENERAL	
COMISIÓN GENERAL	**RESUMEN DE OBSERVACIONES**
Sesión Nº 031 **Fecha:** 27/08/2021 **Link:** **https://www.facebook.com/ComisionSoberaniaAN/videos/1228376060941144/**	
Daniel Tenorio **Experto en ciberseguridad**	• El costo de cibercrimen es equivalente al 1% del PIB mundial, y ha aumentado un 50% desde 2019. • Entre 2019 y 2020, el 70% de las empresas reportó un incidente de ciberseguridad. • Se han datos varias filtraciones masivas de datos. Para el año 2020 los ataques se incrementaron en 358% respecto de años anteriores y 435% desde 2019 (Deep Instint). • El 75% de las organizaciones infectadas con ransomware tienen protección activa. Se estima que habrá un incremento de ataques. • El 91% de los ataques se dan con pishing. El 63% de las instrucciones maliciosas (ataques) en redes son resultado de información como cuentas y usuarios que han sido comprometidos en ataques previos. • En 2020 hubo a nivel mundial 3,21 millones de plazas de trabajo para ciberseguridad no utilizadas. • El entrenamiento y a capacitación son cada vez más necesarios para maximizar la seguridad. Solo el 33% de las organizaciones de América Latina cuenta con un plan de continuidad del negocio. • El 60% de los usuarios cree que sus conocimientos sobre seguridad son insuficientes. • Los ingresos producidos por el ransomware llegarán a 20 billones a fines de 2021. Se deben establecer mecanismos de transparencia hacia el público, se deben establecer mecanismos de control político a la gestión en el ámbito de ciberseguridad. • El gobierno debe desarrollar una política para mejorar los niveles de seguridad nacional. Se deben generar programas de entrenamiento y capacitación continua. Crear un articulado en el cual las Empresas Privadas estén obligadas a notificar sobre las afectaciones sobre seguridad de la información. • Sugiere orquestar cadenas de prevención ante este tipo de ataques.
Ramiro Narváez **Presidente de la Comisión**	• Pregunta como sancionar a quienes cometen delitos informáticos cuando están fuera de nuestro territorio, pues en muchos de casos los delincuentes pueden estar en otro país.

	• Pregunta qué pasa cuando las empresas privadas no han informado a los clientes cuando su información ha sido afectada y no tienen conocimiento, que hacer en estos casos?
Daniel Tenorio **Experto en ciberseguridad**	• Señala respecto del ente rector de seguridad digital que todavía no hay un ente asignado conforme exige la norma. • Es importante definir pronto un ente rector en seguridad digital que no necesariamente sea el ente ejecutor, pueden ser dos entes y esto generaría mayor transparencia, pero de todas formas depende como sea abordada la cyber seguridad en los textos legales. • Finalmente menciona que debemos suscribir los convenios internacionales que establecen estándares de cyber seguridad. Debemos dejar de ser víctimas y empezar a aprender como defendernos.
Sesión Nº 38 **Fecha:** 17/12/2021 **Link**: https://www.facebook.com/ComisionSoberaniaAN/videos/270071441846529/	
Sesión Nº 059 **Fecha:** 24/11/2021 **Link**: https://www.facebook.com/ComisionSoberaniaAN/videos/619432549240476	
Rodrigo Fajardo **Integrante de la Comisión**	• Señala que la legislación nacional debe actualizarse conforme al avance tecnológico. Si bien la sociedad va evolucionando las leyes deban acoplarse a esa realidad. Como hemos visto en las últimas semanas, los ataques cibernéticos han causado zozobra en la población, aumentando la percepción de inseguridad. • El trabajo realizado previo a la presentación del proyecto de ley, se basó en la fiscalización de muchos casos de ataques informáticos a instituciones públicas y privadas, para verificar el daño que se ha ocasionado en las diferentes instancias CNT. • Se ha presentado a la Comisión una resolución para que el Presidente Guillermo Lasso haga los esfuerzos necesarios para suscribir el Convenio de Budapest que tanto lo necesitamos para cooperación internacional para luchar contra los ataque cibernéticos. • El proyecto de ley contiene 16 artículos, 4 reformatorias, 3 transitorias y una disposición final que dan un total de 24 artículos. La materia trata de la seguridad digital desde la perspectiva de los subsistemas de ciber seguridad, ciber defensa y ciber inteligencia, el cual se articula con diferentes instituciones del estado para crear mecanismos y funciones para asegurar y cumplir lo que señala nuestra Constitución de la República al hablar de seguridad Integral. • Con esta ley se crean los subsistemas de ciberseguridad conformado por el Ministerio de Gobierno, Policía Nacional y el Ministerio de Telecomunicaciones y se crean figuras como la de agentes encubiertos, en

	la red, para poder investigar, prevenir y mitigar los incidentes, previniendo hechos delictivos de la seguridad ciudadana. • El Subsistema de la ciberdefensa se encargará de la protección y reacción de la soberanía del Estado en articulación con el Ministerio de Defensa y el Comando Conjunto de las FF.AA., y el subsistema de inteligencia que es un eje preventivo que articula os dos subsistemas antes mencionados para prevenir estos ilícitos. • Todo este sistema está encargado por el secretario del Consejo de Seguridad Pública y del Estado quien bridará información oportuna al Presidente de la República y al COSEPE. • Este proyecto de ley en materia de ciberseguridad establece una nueva competencia a la Superintendencia de Bancos y a la Justa de Regulación Financiera con dos reformas al Código Orgánico Monetario y Financiero para que se establezca un marco de competencias que permita erradicar delitos informáticos en sistemas financieros: así como en diferentes cooperativas, a través de la reforma a la Ley Orgánica de Economía Popular y Solidaria. • Tiene una innovación adicional esta ley al hablar de la Ley de Protección de Datos que creó una Superintendencia como autoridad de Protección de Datos, la cual también debe remitirse la información al Sistema Nacional de Seguridad Digital para su análisis y generación de políticas públicas encaminadas a la protección de nuestros ciudadanos en la red. • Se creó indispensable agregar ciertos delitos informáticos en el COIP por lo cual otorga 180 días desde su vigencia, para reformar en base a lo que establece el Convenio de Budapest, es decir una reforma que se haría al COIP que estaría tipificando ciertos delitos como el ataque a un sistema informático, la interceptación ilícita y ataque a la integridad de los datos, el acceso ilícito a un sistema informático, falsificación informática, fraude informático y abuso de dispositivos. • Muchos países vecinos ya tienen leyes similares y han suscrito el Convenio de Budapest como Colombia, Argentina, Chile y Perú quienes han desarrollado normas, políticas nacionales y estrategias de seguridad digital, ciberseguridad y ciberdefensa, ciberinteligencia y es necesario estar en las mismas condiciones y tener esa cooperación internacional que tanto requerimos. • La seguridad depende de todas y de todos, no podemos pensar desde la concepción antigua: mar, tierra y agua, para incluir al ciberespacio o a la red. • Agradece por el apoyo a esta ley a esta Comisión, a la Bancada de la Izquierda Democrática y a la Asociación Ecuatoriana de Ciberseguridad que nos ha ayudado de forma activa a través de su presidente Gabriel Yumiquinga. • Presenta una moción para dar cumplimiento a la Constitución de la República y solicita que se integre esta Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia, al Código Orgánico de Seguridad del Estado, para lo cual he presentado a moción por escrito

<table>
<tr><td colspan="2">Sesión Nº 64
Fecha: 03/12/2021
Link: https://www.facebook.com/watch/live/?ref=watch_permalink&v=323632899320331</td></tr>
<tr><td>Alejandro Padín Vidal
Experto en Ciberseguridad</td><td>

Trata de realizar una exposición de la ciberseguridad en la legislación europea. Señala que los eventos de ciberseguridad son globales, en primer lugar, porque ocurre en todo el mundo y, en segundo lugar, porque las afectaciones de un ataque se dan en diversas jurisdicciones. Cuentan con una red de abogados a nivel europea y mundial. Hace falta un conocimiento globalizado para entender los problemas de la ciberseguridad, como amenaza global.
Destaca 5 grupos desde donde provienen las amenazas:
1) El crimen organizado: Existen organizaciones de ciberdelincuentes que operan de manera deslocalizada, desde distintas partes de mundo. Hay determinado servicios que se ponen a disposición de terceros, para realizar ciberataques.
2) Hacktivistas: Hacker que atacan empresas, organizaciones o sistemas por razones de activismo.
3) Grupos terroristas: generalmente atacan a infraestructura estratégica. Muchos atacantes están vinculados a servicios de inteligencia de terceros países que los contratan. Incluso se puede llegar a manipular la democracia a través de ataques cibernéticos. Es difícil descubrir cuando un grupo terrorista está vinculado a un Estado, a veces imposible.
4) Estados: Las guerras modernas no se dan con armas sino con ciberataques
5) Casos internos: ataques desde el interior de la propia organización, como filtraciones.
Los objetivos son el sector privado, el sector público, la seguridad nacional y la seguridad el estado.
Los ataques más números son: Malware, Ataques en la web, Phishing, etc.
Características de la ciberseguridad:

Gran dificultad para identificar y perseguir al atacante, lo que desincentiva la persecución del delito.
El sector privado no denuncia, no hay expectativa de reparación.
El sector público no actúa, hay que dedicar demasiados recursos para resultados muy inciertos.
Enormes perjuicios potenciales y reales (Económicos, Operativos y Reputacionales).

El marco regulatorio adoptado en Europa se divide en entre ámbito privado:

Obligaciones de implementar medidas de seguridad.
Obligación de reporte (infraestructura crítica, servicios esenciales, servicios digitales, casos relevantes).

Y en el ámbito público:

Recabar información
Equipos de investigación especializados

El esquema de trabajo es complejo, pero puede ser interpretado: Esquema Nacional de Seguridad (ENS) que contiene principios básicos (Seguridad Integral), requisitos mínimos, medidas de seguridad.
El esquema nacional de interoperabilidad (ENI): Necesidad de que los sistemas sean interoperables.

</td></tr>
</table>

	• Regulación: Normativa "NIS" de Seguridad en Redes y Sistemas (Network and Information Security), Reglamento DORA, Resiliencia Operativa Digital, Reglamento General de Protección de Datos (RGPD), Obligaciones de reporte de brechas de seguridad que afecten a dato personales, Código Penal: Delitos de revelación de secretos, acceso ilegítimo a bases de datos o a información, etc. • Todas estas obligaciones en el ámbito público y privado crean una estructura que permite responder a los ataques informáticos. El problema seguirá en aumento en el futuro, pero esto nos permite afrontar estos ataques. • Los fines de la normativa deben ser la protección de los derechos ciudadanos, la protección de intereses privados, la protección de activos públicos, la protección de infraestructura crítica del Estado, y la protección de las fronteras virtuales del Estado. • Se requiere un sistema de ciber inteligencia. Con la ley de ciberseguridad está muy desarrollada la estructura administrativa. • Como retos del futuro, se debe señalar el fortalecimiento de las organizaciones, contar con una estrategia a mediano y largo plazo y la formación (El eslabón mas débil de la cadena de seguridad se encuentra entre la computadora y la silla".
Ramiro Narváez **Presidente de la Comisión**	• Pregunta, ¿Dónde se centraliza el trabajo de ciberseguridad? Recalca el tema de la interoperatividad, como funciona? Igualmente, como se financia el sistema? Qué hace falta para tener una legislación completa para estar más protegidos, cuál sería el sistema ideal?
José Luis Vallejo **Integrante de la comisión**	• Pregunta el rol de los servidores y empresas que controlan el internet.
Patricia Núñez **Vicepresidenta de la comisión**	• Menciona que le gustaría conocer la experiencia como Comunidad Europea, pues se llegó a un acuerdo de que sea la propia comunidad la que exija los estándares mínimos en materia de ciberseguridad y que resultados han obtenido.
Rodrigo Fajardo **Integrante de la comisión**	• Solicita se aclare cómo_se desarrolle el subsistema de inteligencia y la necesidad de suscribir el Convenio de Budapest.
Alejandro Padín Vidal **Experto en Ciberseguridad**	• Respecto de la estructura señala que ya se cuenta con la normativa nis. Se cuenta con dos columnas, la dirección de ciberseguridad del Ministerio del Interior y la parte de ciberseguridad en Inteligencia. Lo que establece la normativa es que, cuando hay un incidente que puede tener efectos en la seguridad nacional, interviene inteligencia; si es un delito particular, interviene la policía. Existe un Instituto Nacional de Ciberseguridad. • Se debe reportar al CNI los incidentes a la seguridad pública y a las administraciones locales. • La identificación de infraestructura crítica se da por sectores. Es decir, por grandes suministros de electricidad, telecomunicaciones, finanzas, transporte y otros sectores que afectas al funcionamiento del Estado y es la administración central la que identifica las infraestructuras críticas, no las propias empresas para no perder objetividad.

	• En España existe un plan de ciberseguridad con un horizonte a 10 años, con varias líneas de trabajo, proyectos y finalidades. Al final, se dota presupuesto, pero existen recursos escasos. • No hay una dotación en forma de impuestos, sale del presupuesto del Estado. La madurez de la administración y el sistema legislativo son dos indicadores importantes sobre la seguridad de un país. En el caso de la Unión Europea, se aplica la legislación europea en materia de seguridad y la organización del Estado para prevenir y evitar estos problemas. • Debemos tener la certeza que esto no va a parar, pues la tecnología cada vez más va avanzando, de hecho, en los últimos 20 años ha avanzado más rápido que la legislación de cualquier país. Quedan retos como la regulación de la inteligencia artificial, la computación cuántica y otros, y la administración debe estar al tanto de lo que va a ocurrir. • Respecto de las fronteras virtuales y la soberanía, señala que el internet ha supuesto la creación de una nueva jurisdicción, que no está regulada. Los países tradicionales en la ONU tienen fronteras, dentro del esquema aceptado los últimos 100 años, pero con internet todo este desaparece. Lo primero que debemos hacer es reconocer que esto es así, ninguna legislación puede crear fronteras virtuales. La privacidad de los datos es otro eje, (Reglamento General de Protección de Datos), se requiere un principio de soberanía de los datos. • Se debe elevar el nivel de seguridad, sabiendo que es imposible garantizar al 100%. • Como se consigue esta coordinación en la Unión Europea, responde a una historia de coordinación y cooperación entre ciertos países e industrias: BENELUX, Francia-Alemania y en materia de acero. Luego se amplió a más materias y países. Los países han aceptado ceder soberanía en favor de ese ente superior, aquellas materias que son únicas, se regulan de forma única. • Respecto del tema de ETA, señala que no es político y que su opinión personal como ciudadano. Cuando se acabó la dictadura, tuvo como consecuencia el fin de las entidades radical, excepto en el caso de ETA que, aún en democracia, se ha mantenido. Cada vez la legitimidad de su lucha tenía menos sentido, al punto que sus acciones perdieron sentido, por lo que no tenía ni apoyo de la población. Un segundo elemento ha sido la persecución policial, y la detención de las cúpulas, perdiendo así capacidad operativa. Esto vinculado a la ciberseguridad, nos lleva a pensar que hace 10 años apenas había problemas de seguridad en correos electrónicos, ni existía el ciberactivismo. • Destaca que un elemento fundamental es la coordinación. Presenta como ejemplo un ataque a infraestructura estratégica, donde se descubrió que la procedencia era un servicio secreto y el objetivo era solo para recabar información, no se buscaba hacer daño.
Sesión Nº 98 **Fecha:** 08/03/2022 **Link:** https://www.facebook.com/ComisionSoberaniaAN/videos/460527749103271	
José Luis Vallejo	• El concepto de seguridad sistémica es parte de la seguridad del Estado. Nos alegra que en el tratamiento del sistema de seguridad se incluya el tratamiento de este proyecto de ley.

Integrante de la Comisión	• Se ha evidenciado la desarticulación de los organismos competentes, falta de recursos, falta de legislación, etc. el Ecuador está en e puesto 118 de 189 países en materia de ciber seguridad. • Este proyecto tiene 3 bloques: 1) Ciberseguridad: el análisis se basa en la legislación española y EEUU 2) Seguridad Sistémica: desarrolla una propuesta de funcionamiento del sistema de ciber seguridad, banco de alertas, etc. 3) Eje conceptual: contiene todo lo relativo a la tan anhelada seguridad integral.
Sesión Nº 107 **Fecha:** 30/03/2022 **Link:** **https://www.facebook.com/ComisionSoberaniaAN/videos/381314536951147**	
José Luis Vallejo **Integrante de la Comisión**	• Señala que el proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos, fue calificado por el CAL y se encuentra en la Comisión. • Este proyecto se compone de tres ejes fundamentales: ciberseguridad, seguridad sistémica y acceso a la verdad de los hechos, lo que constituye una innovación en términos legislativos. • Vivimos en un mundo de híper conexión, es un mundo en donde la interacción en el ciber espacio crean un entorno de híper registro. Es un mundo donde existen pandemias de desinformación, es un ciber espacio donde Ecuador está en el puesto 119 en cuanto a seguridad, conforme al reporte de seguridad 2020. • En el contexto de lo que se ha señalado anteriormente presentamos un proyecto de ley para garantizar los derechos en el ciber espacio, cuando se accede o intercambia información. • Recalca que hay 95 artículos en su proyecto, más una general y 3 transitorias. El ámbito de aplicación y las definiciones también constan. Se crea una secretaria del consejo de Ciberseguridad, etc. • En relación con el ámbito de aplicación de la ley, puede ser que gracias a la nueva forma de soporte de la información se debe analizar en qué casos debe aplicarse la ley: redes y sistemas de información, infraestructura critica, servicios esenciales dependientes del sistema, servicios digitales, mercados en líneas, etc. • En el caso de existencia de amenazas o ataques, la ley se aplica cuando el ataque se de en redes o cuando la ciber amenaza o infraestructura determinada por el consejo de Ciber seguridad, o cuando se afecte a infraestructura crítica o estratégica. • Una vez se revisa la primera parte del proyecto, el sistema de ciber seguridad incluye a 12 actores, entre los cuales están el ente rector de la política de defensa, de telecomunicaciones, CONARTEL, Fiscalía, Superintendencias, INEC, etc. Siguen los responsables de ciberseguridad de instituciones públicas y privadas. • Los 12 actores se dividen en órganos como el consejo de ciberseguridad, la secretaria de ciber seguridad y la agencia de ciber seguridad, cada uno con sus competencias y atribuciones que procede a describir.

	• Como lo indica el nombre, el proyecto está a disposición de todos, y abierto a todas las posibilidades de perfeccionamiento.
Sesión Nº 132 **Fecha:** 15/06/2022 **Link:** https://www.facebook.com/ComisionSoberaniaAN/videos/383684143592752	
Coronel Victor Nieto **Delegado Ministerio de Defensa**	• Señala que hay poca posibilidad de analizar los tres proyectos de ley, el procedimiento es que se hacen las observaciones a través de la COLEMI y luego se autorizan por parte del Ministro, antes de ser presentados a la Comisión. • señala que por el cambio de autoridades se deben realizar los análisis desde cero, pues los pensamientos estratégicos y críticos difieren, por lo que se necesitan los criterios de la nueva autoridad.
Embajador Germán Ortega **Delegado de la Cancillería**	• señala que a Cancillería le compete el tratamiento de tratados y demás instrumentos internacionales. Se está trabajando para adherirnos al Convenio de Budapest. Si bien los tres proyectos tienen un objetivo común, deberían unificarse para que la Cancillería pueda emitir criterio, en su calidad de integrante del Comité Nacional de Ciberseguridad
Ramiro Narváez **Presidente de la Comisión**	• Pregunta cómo garantizamos que haya una verdadera seguridad digital, necesitamos más aporte de las instituciones vinculadas al sector público y más aún del Ejecutivo. Si desarrollamos la ley solo desde nuestra perspectiva, vamos a tener cambios de última hora y falta de coincidencia en los temas. Hace una cordial invitación para que pongan interés en este tema de fundamental trascendencia, recomienda que formen equipos técnicos para que trabajen de la mano en esta Comisión. Se espera mucho más de las instituciones, pero se necesita una participación más proactiva de parte de todas las instituciones del Estado.
Embajador Germán Ortega **Delegado de la Cancillería**	• Responde asegurando que la Cancillería tiene el mejor deseo de colaborar con la asamblea en estos temas. Asegura que el Canciller ha trabajado en 5 ejes, uno de los cuales es la e-diplomacy, y se están desarrollando los instrumentos legales para hacer realidad esta política.
Andrés Dávila **Delegado Ministerio del Interior**	• Señala que se ha dado el tratamiento y la importancia que el tema se merece, en la nueva estructura del Ministerio está contemplada una unidad para este tema. • En el capítulo 2 del Proyecto de Ley hay una competencia relacionada con ciber seguridad. Es importante señalar que el Comité Nacional de Ciberseguridad ha venido sesionado de manera permanente para desarrollar una política contra la ciber delincuencia y ciber seguridad. Estos términos son muy amplios y más bien sugerimos que se cambie este término por ciber delito. • El ciber delito se encarga de investigar los delitos tecnológicos, mientras que la ciber seguridad previene los incidentes informáticos. Se han

	realizado observaciones técnicas a este documento y venimos trabajando con Policía Nacional.
Fabián Íñiguez **Subsecretario Ministerio de Telecomunicaciones**	• Señala que se ha buscado sentar las bases de una nueva política de ciber seguridad, a través de la constitución del Comité Nacional de Ciber Seguridad, compuesto por el Min Gobierno, Interior, Defensa, CIES, RRII y Presidencia. • Señala que el tema abarca varias aristas, seguridad, defensa, inteligencia, concienciación y ejes transversales en la educación. Recalca que tiene un aporte en el ámbito internacional, firmaron un entendimiento con socios del Caribe y se van a capacitar en un mes. • Menciona que en algunos de los proyectos de ley consultados hay algunas coincidencias, como la gestión de riesgos y la resiliencia, la visión inclusiva, el liderazgo, entre otros. • Se ha tomado contacto con sectores de la academia, las instituciones del sector público, muchos actores del sector privad muy importantes, otras funciones del Estado -como la Asamblea, Fiscalía y Contraloría-. Se han sentado en una mesa, y han creado espacios para luchar contra los ciber delitos. Trabajamos con las superintendencias, quienes nos han dado aportes para este tema. Además, con infraestructura crítica del Estado, los GAD, etc. • El ente rector para la seguridad de la información es el MINTEL, por lo que están dirigiendo el Comité Nacional de Ciberseguridad, pero no es un trabajo exclusivo de este ministerio sino de todas las entidades involucradas.
Ramiro Narváez **Presidente de la Comisión**	• Pregunta, ¿qué estructura es la más adecuada para generar política pública en materia de seguridad digital?, ¿hay un diagnóstico en ciber seguridad en nuestras instituciones?, ¿por qué se junta ciber seguridad y ciber inteligencia, es pertinente, acaso no tiene su propia naturaleza?
Fabián Íñiguez **Subsecretario Ministerio de Telecomunicaciones**	• Destaca que la Ley Orgánica de Telecomunicaciones, en el art. 140, determina que el ente rector en Seguridad de la Información es el MINTEL. La Seguridad de la información abarca ciber seguridad, ciber defensa y ciber inteligencia, se podría requerir la creación de una agencia -de control-. • La segunda pregunta, relativa a los recursos, evidencia que una falencia es la ausencia de estos, se va a dar más fuerza al tema si se encuentra en una ley, por eso llama la atención el proyecto de acceso a la verdad de los hechos, donde la parte de recursos referente a los servicios digitales se debe financiar con un fondo alimentado con el 10% de recaudación sobre servicios digitales. • Este Comité está integrado por ciber seguridad, ciber defensa, ciber inteligencia, pero falta la ciber diplomacia y ciber delitos. Todos se manejan por separado, pero hacen parte de la seguridad digital.
José Luis Vallejo **Integrante de la Comisión**	• Menciona que ahora la diferencia entre la vida pública y la vida publicada es mínima. Se ha hecho el ejercicio de incluir las vulnerabilidades en el proyecto de ley, para lo cual se hace el hacking ético que puede ser realizado por cualquier persona.

Fabián Íñiguez **Subsecretario Ministerio de Telecomunicaciones**	• Se ha aportado en el Comité de Ciber seguridad, para tener un SERT Nacional, que cuando haya alarmas van a poder notificar a las superintendencias, al sector privado y otros.
Marcelo Gómez **Delegado del CIES**	• Expone que el trabajo del CIES ha sido integrar una Comisión Multidisciplinaria para analizar los tres cuerpos de ley. Su análisis ha sido artículo por artículo, cuyo documento con 48 observaciones se remite el mismo día a la Comisión, más allá de ello, solicita la posibilidad de realizar un trabajo a través de un taller donde podamos estar presente los actores y podamos aportar en mayor medida en un trabajo mancomunado. • En los proyectos de se habla de ciber defensa, que ya está regulada en la normativa del Ministerio de Defensa, la ciber seguridad está definida por el Ministerio del Interior, pero la ciber inteligencia es una transversalidad. • La UAFE aporta en función de los casos que se analizan.
Vianna Di María Maino Isaías **Ministra de Telecomunicaciones y Sociedad de la Información**	• Señala que la interacción en línea es una tendencia, los países que tengan la normativa actualizada tendrán un medio ambiente más seguro. • Es vital que la legislación este actualizada, para dar certeza en las transacciones financieras, ciber negocios, etc. • Es importante que estos conceptos acojan las mejores prácticas internacionales porque el ciber espacio es global. • Se debe tener en cuenta el Convenio de Budapest, al que Ecuador se está uniendo, tenemos como país 5 años para hacer las reformas en la normativa penal, para que se adecue a la Convención de Budapest. • La otra mención hace referencia a la estrategia nacional de ciber seguridad que ha sido construida con prácticas internacionales, el lanzamiento será el día jueves, con ayuda del gobierno de Estonia. • Exhorta a los señores asambleístas que ellos como ente regulador deben asegurar una continuidad y las estrategias que debe verse reflejada en la norma.
Sesión Nº 133 **Fecha:** 15/06/2022 Li**nk**: https://www.facebook.com/ComisionSoberaniaAN/videos/446140820677864	
Alexandra Maldonado **Abogada experta en ciberseguridad**	• Expone que la pandemia del COVID ha marcado un punto de inflexión para la senda y ha acentuado nuestra dependencia de la infraestructura digital. • La crisis ha expuesto las deficiencias estructurales de nuestra sociedad y ha afectado muchos sistemas como salud, economía, empleo, y ha tenido un efecto catalizador de cómo hemos manejado la pandemia. • La Ley debe considerar el entorno más disruptivo como es el internet y la infraestructura digital global, que ha hecho posible la provisión de servicios esenciales. • El resultado ha dado profundidad a los ataques cibernéticos y evidencia las falencias del Estado; se han amplificado las deficiencias que tenemos.

	• Las "actividades cibernéticas maliciosas no solo amenazan a las economías, sino también las democracias, libertades y valores, pero sobre todo de la seguridad futura de la que dependerá la capacidad que tengamos para defendernos de conformidad a lo que determine la ley. • Hay que considerar tanto la infraestructura civil como infraestructuras críticas; se debe lograr mayor resiliencia, con un enfoque integral, para que la estructura de base promueva la ciberseguridad y se desarrollen capacidades de respuesta. • Menciona que se debe fortalecer el "enfoque integral digital", con enfoques transversales que permitan crear "resiliencia cibernética y autonomía estratégica", a fin de responder a las brechas de seguridad de nuestro país. Esta norma debe basarse en protocolos de gestión de seguridad digital y protección de la privacidad.
Pedro Ponce **Grupo RADICAL**	• Cualquier ley de ciberseguridad debería abarcar 5 dimensiones: 1) Desarrollar una política y estrategia de ciberseguridad, 2) Fomentar una cultura de ciberseguridad responsable en la sociedad, 3) Crear conocimientos y capacidades en ciberseguridad, 4) Crear marcos legales y regulatorios efectivos y 5) Controlar riesgos a través de estándares y tecnologías. • 1.1.) Desarrollar una política y estrategia de ciberseguridad: Impulsar la estrategia de seguridad cibernética y desarrollar una agenda de seguridad cibernética como un área política importante que determina responsabilidades para los actores clave gubernamentales y no gubernamentales de seguridad cibernética y dirige la asignación de recursos a los problemas y prioridades de seguridad cibernética emergentes y existentes. A Considera: Desarrollo de la estrategia, Contenido de la Estrategia, Implementación y Revisión, Compromisos internacionales. • 1.2) Respuesta a incidentes y gestión de crisis: La Ley debe abordar la capacidad del gobierno para identificar y determinar las características de los incidentes a nivel nacional de manera sistémica. Igualmente dar al gobierno la capacidad para organizar, coordinar y hacer operativa la respuesta a incidentes e integrar a la ciberseguridad en el marco nacional de gestión de crisis. A considerar: Identificación y categorización de incidentes, Organización y existencia de un organismo central autorizado; Integración de la Ciberseguridad en la Gestión de crisis a nivel nacional. • 1.3) Protección de Infraestructuras Críticas: La ley debe impulsar la capacidad del gobierno para identificar Activos de Infraestructuras Críticas (IC), los requisitos normativos específicos de ciberseguridad y la implementación de buenas prácticas por parte de operadores. A considerar: Identificación de IC, Requisitos normativos técnicos y de ciberseguridad de IC, prácticas bajo estándares internacionales. • 1.4) Ciberseguridad en Defensa y Seguridad Nacional: La Ley debe fortalecer la capacidad del gobierno para diseñar e implementar una estrategia de ciberseguridad dentro de la seguridad y defensa nacional; así como promover los acuerdos de colaboración en seguridad cibernética entre las entidades civiles y de defensa. A Considerar: Estrategia de ciberseguridad en las Fuerzas de Defensa, Capacidad de Ciberseguridad de las Fuerzas de Defensa, Coordinación de la Defensa Civil.

	• 2.1) Mentalidad de ciberseguridad: la Ley debe evaluar el grado en que la seguridad cibernética se prioriza y se integra en los valores, actitudes y prácticas del gobierno, el sector privado y los usuarios de la sociedad en general. Una mentalidad de seguridad cibernética consiste en valores, actitudes y prácticas, incluidos los hábitos de usuarios individuales, expertos y otros actores, en el ecosistema de seguridad cibernética que aumentan la capacidad de los usuarios para protegerse en línea. A Considerar: Conciencia de riesgos, prioridad de seguridad; prácticas de ciberseguridad. • 2.2) Confianza y seguridad en los servicios en línea: La Ley debe revisar las habilidades críticas, el manejo de la desinformación, el nivel de confianza de los usuarios en el uso de los servicios en línea en general, y de los servicios de gobierno y comercio electrónicos en particular. A considerar: Alfabetización y habilidades digitales, Confianza del usuario en la búsqueda en línea y en los servicios de gobierno y comer electrónicos, Desinformación; • 2.3) Comprensión del usuario sobre la protección de la información personal en línea: La Ley debe analizar si los usuarios de internet y las partes interesadas dentro de los sectores público y privado reconocen y entienden la importancia de proteger la información personal en línea, y si son sensibles a sus derechos de privacidad. Aspectos para considerar: Protección de información personal en línea. • 2.4) Mecanismo de denuncia: la Ley debe explorar la existencia de mecanismos de denuncia que funcionan como canales para que los usuarios denuncien delitos relacionados con Internet, con o fraude en línea, ciberacoso, abuso infantil en línea, robo de identidad, violaciones a la privacidad y la seguridad, etc. A considerar: mecanismos de información • 2.5) Medios y plataforma en línea: La ley debe explorar si la seguridad cibernética es un tema común de discusión en los principales medios de comunicación y un tema de discusión amplia en las redes sociales. Además, analizar el papel de los medios en la transmisión de información sobre ciberseguridad al público, moldeando así sus valores, actitudes y comportamiento en línea sobre ciberseguridad. A considerar: Medios y redes sociales. • 3.1) Creación de conciencia sobre ciberseguridad: La ley debe enfocarse en la disponibilidad de programas que aumenten la conciencia sobre seguridad cibernética en todo el país, concentrándose en los riesgos y amenazas de seguridad cibernética y las formas de abordarles. A considerar: Iniciativas de sensibilización por parte del gobierno, del sector privado, de la sociedad civil y de los ejecutivos; • 3.2)Educación en ciberseguridad: La Ley debe abordar la disponibilidad y la provisión de programas de educación en seguridad cibernética de alta calidad y suficientes maestros y conferencistas calificados; además, examinar la necesidad de mejorar la educación en seguridad cibernética a nivel nacional e institucional y la colaboración entre el gobierno y la industria para garantizar que las inversiones educativas satisfagan las necesidades den entorno educativo en ciberseguridad en todos los sectores. A considerar: Disposición de oferta educativa en ciberseguridad, Administración y existencia de recursos y marcos de educación en ciberseguridad. • 3.3.) Formación profesional en ciberseguridad: La ley debe abordar y revisar la disponibilidad y provisión de programas asequibles de capacitación profesional en ciberseguridad para crear un cuadro de profesionales en ciberseguridad. Además, analizar la aceptación de la formación en

	ciberseguridad y la transferencia horizontal y vertical de conocimientos y habilidades en ciberseguridad dentro de las organizaciones y como esta transferencia de habilidades se traduce en un aumento continuo de cuadros de mando profesionales de la ciberseguridad. A considerar: Provisión de programas de capacitación en seguridad cibernética; Aceptación de cuadros profesionales en ciberseguridad. • 3.4) Investigación e innovación en Ciberseguridad: La Ley debe dar énfasis en la investigación y la innovación en seguridad cibernética para abordar los desafíos tecnológicos, sociales y comerciales y para avanzar en la construcción de conocimientos y capacidades en seguridad cibernética en el país. A considerar: Investigación y desarrollo en ciberseguridad. • 4.1) Disposiciones legales y reglamentarias: La Ley debe abordar el impacto de la ciberseguridad sobre los derechos humanos. Es necesario profundizar en las diversas disposiciones legislativas reglamentarias relacionadas con la ciberseguridad ya existentes, incluidos requisitos legales y reglamentarios, la legislación sustantiva y procesal sobre delitos cibernéticos y el impacto en los derechos humanos a nivel nacional e internacional. A considerar: Legislación sustantiva sobre delitos cibernéticos, requisitos legales y regulatorios en materia de ciberseguridad del país y de otros países; Legislación procesal sobre delitos informáticos; Evaluación del impacto sobre los derechos humanos. • 4.2.) Marcos legislativos relacionados: La Ley debe abordar los marcos legislativos relacionados con la ciberseguridad, incluida la protección de datos, la protección de los niños, la protección del consumidor y la propiedad intelectual y fortalecerlos. A considerar: Legislación de protección de dato personales, Protección de infancia y adolescencia en línea; Legislación de protección al consumidor; Legislación de propiedad intelectual. • 4.3) Capacidad Legal y regulatoria: La Ley fortalecer la capacidad de las fuerzas del orden para investigar los delitos cibernéticos, la capacidad de la fiscalía para presentar casos de delitos cibernéticos y pruebas electrónicas y la capacidad de los tribunales para presidir casos de delitos cibernéticos y aquellos que involucran pruebas electrónicas. de la misma manera, promover la existencia de organismos reguladores intersectoriales para supervisar el cumplimiento de la normativa específica en ciberseguridad. A considerar: Cumplimiento de la Ley por parte de funcionarios públicos, Capacidad de enjuiciamiento de los fiscales frente a delitos informáticos, Recursos que se deben asignar a los tribunales para enjuiciamiento eficaz, Existencia de organismos reguladores para cumplimiento de normativa específica en ciberseguridad. • 4.4) Marcos de cooperación formal e informal para combatir el delito cibernético: La ley debe abordar la existencia y función de los mecanismo forales e informales que permiten la cooperación entre actores nacionales y transfronterizos para disuadir y combatir a la ciberdelincuencia. A Considerar: Cooperación en materia de aplicación de la ley e intercambio de información del sector público con el sector privado, Cooperación con homólogos extranjeros encargados de hacer cumplir la ley, Colaboración entre el gobierno y el sector de la justicia penal. • 5.1) Cumplimiento de normas: La ley debe revisar la capacidad del gobierno para promover, evaluar la implementación y monitorear el cumplimiento de los estándares y buenas prácticas de ciberseguridad. A considerar: estándares de seguridad TIC, de adquisiciones de software y hardware para

	gestión oportuna de riesgos, ciclo de vida; Normas para la prestación de productos y servicios bajo buenas prácticas y estándares internacionales de ciberseguridad. A cada nivel le corresponde un tipo de regulación, por ejemplo, Estratégico: políticas de seguridad y normas operativas de seguridad; Táctico: clasificación de activos, cumplimiento legal y control de acceso; Operativo: criptografía, seguridad del personal, seguridad física y ambiental, gestión de comunicaciones y operaciones, continuidad de riesgos, brechas operacionales, etc. Debemos asegurar nuestra infraestructura y nuestra data. • 5.2.) Controles de seguridad: La Ley debe exigir el despliegue de controles de seguridad por parte de los usuarios y los sectores público s y privado, y si el conjunto de controles tecnológicos de ciberseguridad se basa en marcos de Ciber seguridad internacionales. A Considerar: Controles de seguridad tecnológica , criptográficos protegiendo datos en tránsito o reposo bajo directrices internacionales. • 5.3. Calidad de software: La Ley debe exigir calidad en la implementación del software y los requisitos funcionales en los sectores público y privado. Además, revisar la existencia y mejora de políticas y procesos para actualizaciones de software y mantenimiento impulsar que se basen en evaluaciones de riesgo y la naturaleza crítica de los servicios. A considerar: Garantía y calidad de software y hardware. • 5.4. Resiliencia de la infraestructura de comunicaciones e internet.: La Ley debe abordar la existencia de servicios de Internet confiables e infraestructura en el país, así como rigurosos procesos de seguridad en los sectores público y privado. Además, revisar el control que el gobierno podría tener sobre la infraestructura de Internet y la medida en que las redes y los sistemas son tercerizados. A Considerar: Confiabilidad de la infraestructura de internet. Monitoreo y respuesta para monitorear la resiliencia de la red en los sectores público y privado. La información, aún cuando este en la nube, debe tener los mecanismos de protección y de encriptación. • 5.5. Mercadeo de ciberseguridad: La ley debe abordar la disponibilidad y el desarrollo de tecnologías de ciberseguridad competitivas, productos de ciberseguros, servicios y experiencias en ciberseguridad, y las implicaciones de seguridad de la subcontratación. A Considerar :Tecnologías de seguridad cibernética en el mercado nacional y si corresponde a nuestras necesidades; Servicios y experiencia en ciberseguridad para organismos públicos y privados; Implicaciones de seguridad de la subcontratación para conocer si se realizan evaluaciones de riesgos para poder mitigarlos en subcontratación de TI (Problema de seguridad en la nube fuera del país por ejemplo); Ciberseguros y regulación de mercado de este tipo de seguros, cobertura y productos asociados. • 5.6. Divulgación responsable: La ley debe establecer un marco de divulgación responsable para la recepción y difusión de información de vulnerabilidades en todos los sectores, y la capacidad para revisar y actualizar continuamente este marco. A considerar: Mecanismos o canales para compartir la información sobre los detalles técnicos de las vulnerabilidades entre las partes interesadas; Políticas y procesos para el responsable de divulgación de fallas de seguridad.

Luis Fernando Enríquez Álvarez **Observatorio de Ciberderechos de la Universidad Andina Simón Bolívar**	• Menciona que falta un glosario de términos, se deben definir conceptos básicos como amenaza, vulnerabilidad, frecuencia de ocurrencia en un período determinado y magnitud (impacto primario y secundario). • Las definiciones de confidencialidad, integridad y disponibilidad debería alinearse a definiciones ya conocidas (Referencias ISO/ IEC 27000: 2018, ISo/ IEC 27005: 2018; Open Group / Factor Analysis of Information Risk). • Indica que una amenaza (o ciber amenaza) por si sola no produce efecto, pues requiere de una vulnerabilidad para determinar la probabilidad de ocurrencia del riesgo. No produce por sí sola impacto ni perdidas de confidencialidad, integridad y disponibilidad, se debe corregir esta definición. • Propone que debería desarrollarse un marco para el fomento de una gestión de riesgos de seguridad de la información y business continuity management, se sugieren considerar la norma 27005ISa y las cinco etapas de la gestión de riesgoss (Seguridad Proactiva). • Menciona que en el Art. 6.5 hay pérdida de autenticidad, revisar conformidad con la Ley Orgánica de Protección de Datos. Las medidas de control haría que se pierda un sistema de autenticidad sino es controlado. • No se hace mención a los CSIRT/CERT. Tampoco se menciona ninguna directriz ni para planes de continuidad de actividades (BCP), ni planes de recuperación de desastres (DRP)} • Armonizar el art. 10.4 de la LEY ORGÁNICA DE SEGURIDAD DIGITAL, CIBERSEGURIDAD, CIBERDEFENSA Y CIBERINTELIGENCIA con la Ley Orgánica de Protección de Datos. Referencia Directiva (UE) 2016/680. • No existe acercamiento al Cy-Var (Cyber Value at Risk), Revisar el artículo 133. 2. (Refencia: World Economic-Forum). Es preciso definir que "fraude" en función de la ley. Ejemplo: No es lo mismo fraude informático que falsificación informática. Refencia (Convenio de Budapest delincuencia informática con fin, delincuencia informática como medio, delitos de contenido). • No existe definición de "delitos digitales", reemplazar or delitos cibernéticos o delitos informáticos. • Incluir a los peritajes informáticos forenses y segmentarlos en especialidades. • Las matrices de riesgo sugieren un análisis cualitativo, considerando en la actualidad como altamente subjetivo; se sugiere incluir otras metodologías de análisis de riesgos, en particular cuantitativo y semi cuantitativo. • La auditoría de seguridad no debería ser solo anual, dependen del tipo de institución y el perfil de riesgo, y deben ser realizadas por auditorías técnicas y organizacionales. • Se debe precisar en las violaciones de seguridad de datos, no se puede confundir la gestión de riesgos de seguridad de la información con la gestión de riesgos de la protección de derechos libertades. Es importante tener la multidimencionalidad del riesgo. • Se refiere a un bando de alertas, pero falta una definición en el caso que se refiere a generar alertas en sistemas de detección y prevención de intrusos (IDS/IPS). • Ciberamenaza no produce daño sin que exista vulnerabilidad.
Sesión Nº 157 **Fecha:** 24/08/2022	

Link: https://www.facebook.com/ComisionSoberaniaAN/videos/478108654138566	
Diego Urbina **Asesor en materia de Política Pública Amazon Watch Service**	• Agradece la apertura y la transparencia. Antes de entrar en detalle va a presentar la empresa, que inició en 1994. Esta empresa fue creciendo y se convirtió en una empresa global para lo que desarrollo tecnología para sus propios servicios, pero que luego se vendió al público. En 2006 surge el concepto de información en la nube. • ¿Que significa computación en nube? Son servicios en internet de pago por uso de servicios de computación, bases de datos, almacenamiento para empresas privadas y públicas. Estos servicios tienen beneficios, uno de ellos, la agilidad en la cual uno puede ofrecer un nuevo servicio a medida que aparecer una necesidad; la elasticidad es otro beneficio, pues permite manejar más información, por ejemplo, en las elecciones, se requieren servidores con una gran potencia, pero que luego de las elecciones los servidores quedan subutilizados. La nube, solo se paga por los servicios que se están usando de manera efectiva a diferencia de cuando uno necesita servidores en la institución, con personal, mantenimiento, actualización, etc. Se paga por el uso. • El hecho de que no tengamos a nuestro personal verificando los servidores permite hacer más eficiente el uso del personal. Cambios que se pensaban en 5 años, se hicieron en 5 meses por la pandemia, muchas veces los trámites prepandemia se redujeron al volverse digitales. Los servicios son más rápidos gracias la nube. Ecuador está avanzando de manera acelerada en transformación digital. Se deben aterrizar en objetivos concretos, se ha aprobado una estrategia nacional de ciberseguridad. Lo que se está haciendo en esta comisión es muy valioso. • Los tres proyectos deberían ser unificados en uno solo, se debe modificar el art. 146 de Código Ingenios que regula la ubicación de los servidores de las entidades públicas. Esto no fomenta una transformación digital acelerada sino más bien bloquea los servicios para el ciudadano. En materia de seguridad, en general, la nube es el ambiente más seguro para este tipo de datos. Manejamos datos de defensa, inteligencia, salud entre otros que tienen los más altos estándares de seguridad. Cualquier estándar de seguridad es aplicable a todos los clientes. En materia de ciberseguridad, el ambiente óptimo para conservar datos en la nube. • Muchas veces uno piensa que el proveedor va a poder ver la información del cliente, pero bajo los mecanismos de seguridad impiden que se vea esa información. Si hubiera un ataque los servidores están en diferentes lugares. Ofrece un webinar sobre ciberseguridad, totalmente agnóstica para que conozcan la seguridad en la nube. • trabajamos en un modelo de gestión de responsabilidad compartida. Nosotros nos encargamos que los servidores y la infraestructura sean lo más seguros posibles. Mientras que la seguridad en la nube depende de los usuarios. Hay diversas formas de proteger los datos, pero nunca se pierda la propiedad de los datos, no podemos entrar y mirar los datos. Los datos se encriptan de manera automática, tanto cuando están en tránsito como cuando están en uso. No se comparte el espacio, lo que se comparte son las credenciales globales de seguridad. Si Ecuador requiere un ISO específico, todos los clientes se benefician de eso.

	• En una protesta social se quemaron los servidores de una municipalidad, ellos pensaron que teniendo los datos en sus servidores estaban seguros, pero no era así. Uno pensaría que es más fácil cuidar los datos porque los ven, pero solo compañías como AMAZON pueden ofrecer los niveles de seguridad que da una economía de escala. Nunca se pierde la propiedad de los datos, entonces es bastante más seguro y en cuanto al pago por uso, depende del tipo de servicios. Tenemos más de 200 servicios, pero hay servicios de inteligencia artificial. Hay muchos casos interesantes en ciberseguridad. Una vez que los datos existen y el dueño de los datos quiere hacer uso de ellos, se pueden hacer servicios interesantes. El tema del Código Ingenios implica que los servidores no estén localizados acá, pues eso no implica más seguridad. Pueden ser víctimas de ciberataques fácilmente, con un esquema de seguridad más poderoso. • Hay una política de nube primero, es decir, que los servicios que aparecen sean previstos desde la nube. Los vehículos de contratación de tecnología tienen distintas características, donde las entidades de compras públicas lo hacen por bienes Acá el pago es por uso y sería una buena práctica de seguridad. Ecuador está avanzando en la Ley y se requieren marcos de regulación de ciberseguridad basados en estándares internacionales, no vamos a inventar algo nuevo. Se requiere una ley de clasificación de datos, no todos se manejan con el mismo nivel de seguridad. • Las políticas deben ser de obligatorio cumplimiento, y debe haber una entidad que sea capaz de controlar. El MINTEL ha tenido la apertura para recibir comentarios de diversos actores y observa las mejores prácticas internacionales. Ellos mencionan la cooperación a nivel internacional y la necesidad de ajustarse a los estándares que ya existen. ¿Qué faltaría? Aterrizarla en objetivos más concretos, como objetivos de cumplimiento, una agenda de transformación digital. • Diego Álvarez: el año pasado se publicó la Ley de datos personales, pero en términos técnicos es una entidad más cercana al manejo de la información; se va a crear una superintendencia de control de datos. Esto tiene un alto componente técnico, pero se deben atribuir competencias en materia de ciberseguridad. La tecnología avanza más rápido que la regulación, pero no solo debemos regular las malas experiencias, sino también lo que se viene, el futuro. Desde el momento que nos levantamos usamos información en la nube.
Sesión Nº 160 **Fecha:** 31/08/2022 Li**nk**: https://www.facebook.com/watch/live/?ref=watch_permalink&v=1191674628065676	
Humberto Arthos **Delegado Agencia de Regulación y control de las Telecomunicaciones (ACOTEL)**	• Señala los conceptos relacionados a las leyes: ciberseguridad, ciberinteligencia o ciberdefensa. Hay algunas palabras que no significan lo mismo para la academia, las leyes o los técnicos. La ciberseguridad hace relación a la protección de activos y usuarios. La ciberinteligencia busca realizar actividades de inteligencia en ciberseguridad. • ¿En qué se diferencian los tres conceptos? La ciberseguridad se rige por civiles y busca que los activos digitales mantengan su valor, la

	ciberinteligencia busca como se procesan y analizan los datos y la ciberdefensa guarda relación con la protección de la soberanía. • Así mismo, hace referencia al ECUcert., ¿qué hace? ¿A qué se dedica? Se creó en 2014, nuestro objetivo son los prestadores de servicios de telecomunicaciones. Nuestra misión es brindar el apoyo a la comunidad objetivo a través de los servicios que facilitamos y que son reactivos, proactivos y de valor agregado. • Explica los canales de comunicación a nivel internacional: OEA, APWG, Clean MX, etc. Si bien no están calificados como un CERT nacional, si colaboran con el Estado. Tampoco están certificados para ser un CERT en el área bancaria. • Realiza sus observaciones a los proyectos de ciberseguridad, respecto de los que hay observaciones puntuales: 1. Primero se debería homologar los artículos que tienen definiciones, para evitar la contraposición con leyes vigentes (datos, telecomunicaciones, normativa internacional, etc.) 2. La estructura del sector y de la nueva entidad debe ser trabajada entre todas las partes involucradas. 3. Definir que institución debe gestionar las ciber amenazas. 4. Se debe tener una capacidad sancionatoria, sin perjuicio de las capacidades de ARCOTEL. 5. Se debe definir las funciones del EcuCERT, pues MINTEL no tiene competencias sancionatorias. 6. Se debe alinear a la Estrategia Nacional de Ciberseguridad. 7. Se deben revisar los requisitos para que la persona seleccionada como directora de la nueva institución sea la más idónea tanto por experiencia como formación. • Respecto del proyecto de Rodrigo Fajardo: 1. Homologar los conceptos de infraestructura crítica. 2. Los términos de ciberseguridad, ciberdefensa, ciberinteligencia, son diferentes. 3. No es necesario que una sola agencia maneje las tres funciones: ciber inteligencia, ciber defensa y ciberseguridad. • Respecto del Proyecto de José Luis Vallejo: 1. Se debe realizar una definición clara de los términos utilizados. 2. No se puede garantizar la ciberseguridad, es algo que evoluciona cada día y lo que sirve para mitigar una cosa mañana no sirve. 3. Es factible proteger los activos digitales, pero no el ciberespacio como tal. 4. Una ley no garantiza la cooperación internacional, deben buscarse espacios y mecanismos de cooperación. 5. Se deben considerar las siguientes definiciones: autenticidad, integridad, etc. 6. La emisión de alertas no puede estar sujeta a procesos burocráticos. Se debe detallar claramente lo relacionado a la verdad de los hechos.
Sesión Nº 162 **Fecha:** 07/09/2022 Li**nk**: https://www.facebook.com/ComisionSoberaniaAN/videos/744584409937308	

Jonathan Ramos **Docente de Derecho Penal UCE y representante de la Asociación Académica ecuatoriana de Derecho e Informática**	• Sin perjuicio que el COIP ya establece parámetros para la construcción de ciertos tipos penales, procede a analizar el contenido de los proyectos de ley. El derecho a la seguridad ciudadana es un derecho poco regulado, por ello es importante abordar la construcción del proyecto desde los estándares internacionales. Cuando se regula la ciber delincuencia, se plantea la pregunta que bienes jurídicos protegidos entran en regulación. Nuestra legislación protege la integridad de los sistemas informáticos. El derecho penal no protege derechos constitucionales, ni protege bienes jurídicos, es decir, se activa una vez que se da la conducta. La escuela alemana habla de prevención general, por el carácter gravoso de la pena. ¿qué es información sensible? Es un concepto jurídico indeterminado. • El ciber espionaje sirve para apropiarse de información sensible. El COIP tipifica el acceso al sistema, no se necesita un resultado como tal. Qué pasa si alguien vende un sistema para acceder a información sensible, nada porque no tenemos el delito de abuso de dispositivos. • Todos los organismos que conforman el sistema de seguridad digital son públicos, en un sistema debe mantenerse la participación de la ciudadanía, para que pueda acceder a información que no sea confidencial o reservada legalmente. • No tenemos un instrumento vinculado con Ciberdelincuencia, se debe especificar qué tipo de información está protegida. El Convenio de Budapest da la posibilidad a los estados que se entregue la información inmediatamente, pero esto podría acarrear una violación de DDHH. ¿Qué pasa si dentro de la información se violentan derechos fundamentales? Los textos normativos deben estar armonizados a principios y derechos constitucionales, se recomienda cambiar la denominación. • Si se borra información, o se suprime información, es diferente. La lesión depende si se puede o no recuperar la información. • ¿Qué pasa si el delito se produce en otro país? No tenemos convenios para hacer cooperación internacional. Lo primero que se debe garantizar es la existencia de disposiciones materiales que permitan la lucha nacional e internacional de estos delitos. • No existe el concepto de dato personal actualmente. • Respecto del registro de datos informáticos almacenados, se requiere autoridades competentes para conservar los datos, que se determinar la responsabilidad en un hecho delictual. Respecto de la interceptación de datos, señala que la asistencia de un proveedor internacional sin autorización formal, se podría dar sin pedido de juez. No se debe esperar que otro estado solicite la información, si se da una investigación se debe generar la información de manera espontánea. • Debemos estar a la par para reducir la brecha digital con los países desarrollados. Esperamos que se puedan tomar en consideración en la construcción de la norma estos principios.
Sesión Nº 164 **Fecha:** 09/09/2022 Li**nk**: https://www.facebook.com/ComisionSoberaniaAN/videos/462078729165709	
Marcelo Gómez **Delegado del**	• señala que los dominios de intervención del Estado son mar, aire y espacio, pero ahora se incorpora como otro dominio el ciberespacio. La SNAIN y

Centro de Inteligencia Estratégica	MINTEL generaron el esquema de seguridad gubernamental, desde 2013. Este tratamiento y la propuesta se proponía en cada uno de ellos de manera similar, otro punto importante de estas propuestas es que constituyen un punto de partida para las infraestructuras criticas para la seguridad digital, además de establecer mecanismos permanentes para acceder a certificaciones en materia de seguridad del ciberespacio. Algunas desventajas lo corregimos, que eran tres proyectos de ley que no mantienen una relación directa con el ámbito de aplicación de la ley como es "la verdad de los hechos". Por otra parte, el establecer tareas operativas en estas leyes debería esta en normativa secundaria. • Ponemos a consideración de ustedes que en base de los documentos base para la elaboración de una ley, como decretos ejecutivos y la Ley de Seguridad Pública y del Estado. E debería integrar a la Secretaría Nacional de Seguridad Pública y del Estado. Finalmente, se deben mejorar algunos términos como "garantizar", que esto es preciso. • la ciberdefensa le corresponde al MIDENA. Por la experiencia en el país, en ciberinteligencia, ciberdefensa y ciberseguridad, se debería compartir criterios respeto a la propuesta que se ha realizado.
Ramiro Narváez **Presidente de la Comisión**	• Pregunta ¿el CIES tiene un CERT? ¿Cuál es el nivel de articulación con ARCOTEL?
Marcelo Gómez **Delegado del Centro de Inteligencia Estratégica**	• Responde El CIES no tiene un CERT como tal. Han levantado protocolos para mejorar la infraestructura critica, pero no están encargados de actuar a través de un centro de inteligencia estratégica. El trabajo coordinado con MIDENA y con el personal del CIES. • Respecto de ARCOTEL, la comunicación es con el MINTEL y forman parte de la Comisión Nacional de Ciberseguridad, a la que asisten y aportan permanentemente. La Estrategia Nacional de Ciberseguridad ha generado mecanismos adicionales para poder llevar adelante los 6 ejes propuestos en la misma.
Ramiro Narváez **Presidente de la Comisión**	• Pregunta ¿en la ley se plantea la opción de que tengan un CERT, no lo requieren?
Marcelo Gómez **Delegado del Centro de Inteligencia Estratégica**	• Necesitamos un CERT, el país necesita tener un CERT y el CIES requiere tenerlo. La normativa actual no nos permite, se debe determinar los recursos necesarios y que entidades deben formar parte para contar con aportes de las capacidades de otras instituciones.
Ramiro Narváez **Presidente de la Comisión**	• Pregunta ¿Ha habido algún incidente relativo a ciberseguridad?
Marcelo Gómez **Delegado del Centro de Inteligencia Estratégica**	• Contesta que ha habido intenciones de vulnerar infraestructura crítica y hemos apoyado a Cancillería con ciertas novedades en el servicio.

Sesión Nº 209 **Fecha:** 23/02/2023 Li**nk**: https://fb.watch/jgqUCQTFIh/	
Patricia Núñez **Vicepresidenta de la Comisión**	• La Comisión realizó un total de 8 sesiones en las que avocó conocimiento de estos proyectos e invitó a la academia, sector privado, observatorios, organizaciones de la sociedad civil y expertos internacionales, a fin de qué brinden sus aportes y sugerencias, a fin elaborar el borrador de texto unificado. • Posteriormente, la Comisión organizó un amplio debate con las instituciones involucradas en la temática de Cyberseguridad, entre otras participaron el Ministerio de Defensa la Policía Nacional el CIES el Ministerio del Interior el Ministerio de Telecomunicaciones, entre otras que en un total de 10 mesas de trabajo revisaron el borrador de texto previo al 1er debate, mismo que cuenta con 79 artículos, que abordan la estructura en Sistema Nacional de Seguridad Digital en 4 subsistemas: 1.- El Subsistema de Ciberseguridad ciudadana, encargado de resguardar la seguridad ciudadana y protección interna en el ciberespacio, como por ejemplo ante delitos informáticos como el robo de información personal, el acceso no autorizado a archivos o el robo y destrucción de archivos, entre otros. 2.- El Subsistema de Ciberdefensa, encargado de la defensa, , respuesta y recuperación frente a riesgos, amenazas, incidentes en el ciberespacio cuando tengan relación con la soberanía del Estado, como ataques a la información de sus instituciones públicas. 3.- El Subsistema de Ciberinteligencia, responsable contar con información para identificación y alerta ante amenazas que afecten la seguridad digital de la infraestructura estratégica, infraestructura crítica digital y los servicios esenciales del Estado. 4.- Y, finalmente, el Subsistema de Ciberdiplomacia, que articulará acciones cuando se requiera la cooperación internacional para la detección oportuna y neutralización de amenazas, riesgos e incidentes; la prevención y combate al ciberdelito y la cibercriminalidad; la defensa de la soberanía y la seguridad integral; la política exterior y movilidad humana; y, la promoción del Ecuador en el exterior. • Señala que es importante recalcar que el Ecuador es uno de los países más vulnerables de la región en materia de Ciberseguridad, los estándares internacionales establecen una serie de requisitos técnicos y legales a fin de calificar el estado de la seguridad digital de un Estado, entre otros, el contar con una ley que regule la temática. Otros países como Colombia Uruguay y Argentina cuentan incluso con centros de respuesta a incidentes informáticos certificados internacionalmente. Nosotros todavía no hemos desarrollado las

	herramientas necesarias, técnicas y de talento humano, para tener mayores niveles de seguridad en nuestro acceso al ciberespacio. Esta ley va a coadyuvará a este objetivo que sin duda será uno de los grades desafíos del Ecuador mejorar el Estado de la ciberseguridad en el país. Pregunta a la asesoría de la Comisión, respecto del ámbito, ¿Cómo se puede determinar que es una amenaza, riesgo o incidente en redes? Para evitar que queda a discrecionalidad, a través de algún parámetro que nos permite identificarlos.
Melania Carrión **Asesora de la Comisión**	En el art. 5 se definen las amenazas, hay que entender la naturaleza de este tipo de eventos que se dan en el ciberespacio. En general, cuando uno advierte los mecanismos y procesos para el abordaje de todo lo que entra en la categoría de incidentes, como podrían ser eventos, la falla de un sistema un ataque a un sistema o una crisis en el ámbito de la seguridad digital, estos están asociados a la gestión de riesgos. • Una de las cosas que se había determinado previamente es que esta ley va a tener algunos elementos muy similares a lo que se aborda en la ley de gestión de riesgos. • Si bien los riesgos antrópicos o naturales son amenazas producto de vulnerabilidades no gestionadas, lo mismo sucede en el ámbito de la seguridad digital. • Los sistemas, las estructuras, pueden verse vulnerados, se genera una amenaza y si no hay una adecuada gestión puede darse un incidente, este evento puede ser un ataque o un error de funcionamiento del sistema o una crisis en el orden de la seguridad digital. • Cada subsistema va a tener un proceso sustantivo que va a permitir llegar a esa precisión. En el texto inicial se hacía referencia ataques, crisis digitales, etc. pero se explicó que existe un proceso para notificar cuando un incidente es un ataque o si luego de un triaje se determina que no es un ataque, para ello la ley determina procesos para gestionar estos incidentes, para lo cual se crea un Centro Nacional de Respuesta a Incidentes que va a tener su propia regulación. • El artículo menciona de forma genérica el ámbito conforme a la técnica legislativa, solo determina la materia y el ámbito territorial de aplicación, señalando los actores, tanto públicos como privados. Evidentemente de los hechos que se dan en el ciberespacio cuando las infraestructuras estén en el ámbito ecuatoriano o bajo su jurisdicción, como en embajadas, importante pues no existe el ámbito territorial en el sentido físico y cuando una determinada circunstancia pueda surgir efectos en el Ecuador. En uno de los proyectos de ley se desarrollaba un ámbito más detallado relacionado con actividades protegidas para evitar que se extienda de manera amplia a todas las actividades, por ejemplo, si una persona tiene un problema en su computadora no debe activar todo el sistema, pero se identifican las actividades protegidas.
Patricia Núñez **Vicepresidenta de la Comisión**	• En el art. 3, numeral 9, dice promover la confianza para el intercambio de información y la gestión de conocimiento de seguridad en el ciber espacio. Cuando hablamos de intercambio de información podríamos correr el riego

	que se atente contra los derechos individuales ¿Cómo logramos garantizar eso?
Melania Carrión **Asesora de la Comisión**	• En el ámbito se había especificado que esta ley, cuyas disposiciones son de orden institucional y no desarrolla de manera sustantiva o adjetiva los procesos específicos, hay un subsistema de ciberseguridad que está regentado por el Ministerio de Interior y que tiene como objetivo evitar la vulneración de derechos, a través de los procesos que lleva a delante la unidad específica de ciberdelitos, es decir esos procesos van a seguir actuando, conforme a la ley, no es que se altera o modifican los procesos en los que estas entidades deben actuar. • ¿Cuál es la naturaleza del proyecto de ley? Es institucional y busca articular a las distintas entidades y los esfuerzos que realizan para poder responder en caso de que existiera una amenaza a las infraestructuras digitales o que existiera algún problema en el ámbito de sus competencias. • Este ejercicio de promoción es con el objetivo de que cada uno de los subsistemas, en cada uno de sus ámbitos de competencia, puedan generar este intercambio de información. Bajo ningún sentido la ley otorga facultades más allá de lo normado en la legislación vigente, por ejemplo, el COIP. Esta ley no desarrolla ni limita estas facultades, sino que únicamente las circunscribe al ámbito de la seguridad digital por lo que no se verían afectados los derechos y garantías establecidos en la Constitución.
Sesión Nº 211 **Fecha:** 24/02/2023 Li**nk**: https://fb.watch/jgqYLXqRaz/	
Melania Carrión **Asesora de la Comisión**	• Menciona que el cumplimiento de las funciones se da a través de los subsistemas, mismos que ejercen la rectoría y capacidad de control, como la Agencia Nacional de Regulación y Control. • La Ley va a dar temas generales que permitiría que todos los integrantes del sistema puedan responder a los integrantes del sistema. Se puede clarificar el numeral 1 porque no es para todos los servicios del Estado. No esperar que sea alguna otra entidad la que realicen la evaluación de vulnerabilidades. Todos los numerales tienen que ver con cuestiones de carácter genérico.
Patricia Núñez **Vicepresidenta de la Comisión**	• ¿Por qué se da la Rectoría al Ministerio de Telecomunicaciones?
Melania Carrión **Asesora de la Comisión**	• Responde que este fue un tema ampliamente debatido en las mesas técnicas, para definir quién va a asumir esta rectoría. A más de los tres proyectos, se consideró las mejores prácticas y estándares internacionales, derecho comparado y la estrategia y el plan nacional de seguridad digital. • Agrega que el proyecto del Asambleísta Fajardo se tomó como referencia, porque en el caso de las instancias colegiadas, si no se determina una entidad rectora, el trabajo se diluye. Se consideró que debía haber un ente rector, podía ser de seguridad, sí, pero había el problema de la coordinación. La Reflexión se dio respecto a si podría ser la Secretaría de Seguridad

	Pública, se debería reformar la Ley de Fortalecimiento Institucional y Seguridad Integral. • Expone que sería contraproducente otorgarle la rectoría a una secretaría que no tiene capacidades técnicas instaladas. ¿Qué otra entidad quedaba? Al SNAI, MDI, MIDENA, CIES o la Policía que no tendrían la rectoría, pues no es su ámbito. Incluso el CIES entrega insumos, pero no toma decisiones. Ahí viene al gran problema de las iniciativas de ley, que ninguno de los proyectos es de iniciativa del Ejecutivo, por lo que no se puede crear una institucionalidad que cree gasto público. • Alega que no se podría crear una agencia en esta ley, por no ser de iniciativa del Ejecutivo. Quedaba en consecuencia, pensar en una de las entidades que ya ejercía rectoría en el tema. Los ministerios que tienen la experticia tecnológica son los que deben asumir esta rectoría. La otra opción es que sea una de las entidades del sector seguridad, que no sea una que no regule un subsistema, porque no sería pertinente tener una entidad que regule todo el sistema y, a la vez, un subsistema.
Patricia Núñez **Vicepresidenta de la Comisión**	• Se puede incluir a la Corte Nacional en lugar del Consejo de la Judicatura.
Melania Carrión **Asesora de la Comisión**	• Señala que no sería necesario en razón de que esta ley no establece nada en materia jurisdiccional.
Patricia Núñez **Vicepresidenta de la Comisión**	• ¿Como logramos que no se filtre la información?
Melania Carrión **Asesora de la Comisión**	• Responde que se ha señalado en varios artículos que se respetarán los niveles de clasificación. • Expone que las entidades deben informar, alertar, presentar información estadística, etc. Pero no se va a dar al detalle información sobre x caso, salvo que así lo determine el COSEPE o el Comité. Hay varios artículos que buscan transversalizar cómo se compartimenta la información y se da su manejo adecuado.
Patricia Núñez **Vicepresidenta de la Comisión**	• Se habla de realizar un análisis de vulnerabilidades en ciberseguridad ¿esto es solo para las entidades relacionadas a ciberseguridad o es para todas las entidades que conforman los subsistemas?
Melania Carrión **Asesora de la Comisión**	• No necesariamente debe hacerlo el ente rector, pero se puede clarificar pues cada entidad que pertenece al sistema tiene que hacer su propio análisis de vulnerabilidad, no es una facultad del ente rector el cual solo emite las directrices de política.
Patricia Núñez **Vicepresidenta de la Comisión**	• ¿En el tema de suscribir convenios interinstitucionales, no sería competencia de un subsistema?

Melania Carrión **Asesora de la Comisión**	• Se reconoce esta potestad ya existente, por ejemplo, la Policía Nacional tiene acuerdo con sus pares y son negociados directamente con las instituciones.
Jorge Pinto, **integrante de la Comisión**	• Consulta si hay contraposición con la ley de inteligencia.
Melania Carrión, **asesora de la Comisión**	• Se podría especificar que los requerimientos de información se harán conforme a la normativa vigente o por su ley específica, en este caso el proyecto de ley de inteligencia que está en tratamiento en la Comisión

Fuente: Matriz de sistematización de comisiones generales previo al Informe para primer debate.
Elaboración: Comisión Especializada Permanente de Soberanía Integración y Seguridad Integral.

2.2.2. Observaciones institucionales y ciudadanas remitidas por escrito

Durante el proceso de socialización previo a la elaboración del Informe para Primer debate del Proyecto de Ley, se recibió una decena de comunicaciones por escrito con observaciones generales y puntuales a los proyectos de Ley unificados, conforme consta en la siguiente tabla:

Tabla 2: Observaciones institucionales y ciudadanas remitidas por escrito

No.	INSTITUCIÓN ORGANISMO ORGANIZACIÓN CIUDADANO	ASPECTOS OBSERVADOS
	Coronel (SP) Fausto Cobo, Director General de Centro de Inteligencia Estratégica Oficio Nro. CIES-CIES-0108-2022-OF[1]	• **Observaciones Ley de Seguridad Digital[2]:** - Sugiere cambiar "Consejo de Seguridad Integral del Estado" por "Consejo de Seguridad Pública y del Estado" - Sugiere una nueva definición de la palabra ciberespacio: "Es un mundo no físico, sin límites, donde cualquier persona puede estar interconectada, utilizando software, con una conexión a la red de tal manera que pueda interactuar con el mundo virtual sin barreras" - Respecto de la organización del Sistema de Seguridad Digital, señala que "Se debe analizar la necesidad de contar con 4 subsistemas, lo suficiente debería ser 3, y Ciberseguridad, Ciberdefensa y Ciberinteligencia" - Señala que el CIES ya tiene una estructura para ciberseguridad por lo que sugiere cambiar "Seguridad Digital de la Secretaría de Inteligencia" por "Ciberinteligencia del Centro de Inteligencia Estratégico" - Sugiere cambiar "Plan Nacional de Seguridad Cibernética" por "Plan Nacional de Seguridad Digital"

[1] ANEXO 1: Oficio Nro. CIES-CIES-0108-2022-OF
[2] ANEXO 2: Observaciones Ley de Seguridad Digital

		- Recomienda agregar el siguiente texto: "Coordinar con el componente de Ciberinteligencia respecto de la información de los componentes de Ciberseguridad y Ciberdefensa" - Respecto del Comando de Ciberdefensa de las Fuerzas Armadas, en lo relativo a sus funciones, sugiere: "considerar la participación de entidades a nivel ministerial de la Defensa" - Realiza la revisión de propuestas gramaticales • **Observaciones Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa, Ciberinteligencia[3]:** - Señala que el CIES debe formar parte de las funciones del Estado con competencia en materia de seguridad digital - Señala que "la forma cambiante y evolucionada en la cual desarrollan las actividades en el ciberespacio, requiere una revisión permanente de la normativa lo cual se ajustará a las necesidades del país" - Respecto del Sistema de Seguridad Digital señala que "El establecimiento de la presente - ley generará doctrina de la terminología utilizada en el Ecuador, por ejemplo en algunas teorías se establece que el ciberespacio corresponde únicamente a los elementos de tecnología que permiten que se forme parte del Internet, otras indican que es cualquier elemento que se conecta a una red de datos. Las crisis se gestionan y lo indicado en el objeto es parte de un proceso, adicionalmente indicar que la recuperación de la información es parte de un proceso que tiene que ver con la gestión de la contingencia. • Respecto del ámbito de aplicación se quiere incluir la palabra "formulación" de política pública. • Sugiere incluir la siguiente definición. Ciberamenaza: Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste. Ciberataque: Uso del ciberespacio para atacar a los sistemas y servicios presentes en el mismo o alcanzables a través suyo. El atacante busca acceder sin autorización a información, o alterar o impedir el funcionamiento de los servicios. Infraestructura Crítica: Instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales. Servicio Esencial: Servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas. • Respecto de los principios recomienda incluir los siguientes: Confidencialidad, Integridad, Disponibilidad, Proactividad. • Respecto de las funciones del Sistema de Seguridad Digital, propone el siguiente texto: los órganos e instituciones del Sistema de Seguridad Digital deberán establecer la normativa que permita precautelar la seguridad en el ciberespacio, que genere la información para que, posterior al análisis correspondiente habilite la toma de decisiones necesarias para preservar el funcionamiento de los activos que almacenan,

[3] ANEXO 3: Observaciones Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa, Ciberinteligencia

		procesan, transmiten y tratan información digital de las instituciones públicas del Estado ecuatoriano. • Respecto de la rectoría del Sistema nacional de Seguridad Digital, propone que la misma no se encuentre en manos del Consejo de Seguridad Pública y del Estado, sino a través de su Secretaría General, indicando que el COSEPE no puede tener rectoría por las atribuciones y competencias que se tienen establecidas, es un entorno que no maneja recursos o puede emitir política. Se debe precautelar que los entes competentes en la seguridad aporten directamente en el sistema, otros entes serán de apoyo a la consecución de los objetivos". • El Plan de Seguridad Digital debe ser elaborado por los miembros del Consejo y aprobado por el mismo como ente rector. • Respecto de las funciones y atribuciones, propone el siguiente texto: 2) Aprobar la política pública de las instituciones en materia de seguridad digital, que se definan mediante el Sistema Nacional de Seguridad Digital considerando los subsistemas de ciberseguridad, ciberdefensa y ciberinteligencia. (…) 4) Supervisar los informes emitidos por las entidades que conforman el Sistema Nacional de Seguridad Digital para la protección de las infraestructuras críticas. (…) 7) Dar seguimiento y presentar informes a la o el Presidente de la República y al Consejo de Seguridad Pública y del Estado sobre los hechos delictivos que han atentado o podrían a la Seguridad Digital del Estado. • Respecto de la conformación del Subsistema de Ciberseguridad, propone el siguiente texto: El Subsistema de Ciberseguridad estará conformado por: Un delegado de la Secretaría Nacional de Seguridad. Ministerio de Gobierno. Centro de Inteligencia Estratégica. En relación con las funciones del subsistema será ciberseguridad además de las de normar, articular, y proponer normativa que permita preservar un nivel de seguridad digital, establecer un sistema de evaluación y control que permita mejorar de manera continua el nivel de seguridad digital de las instituciones públicas. • Propone un texto nuevo. Funciones del Delegado de la Secretaría Nacional de Seguridad.1. Cumplir y hacer cumplir con las políticas públicas, estrategias, planes emitidos por el ente rector de la materia.2. Articular y proponer las acciones necesarias para definir y mantener actualizado el catálogo de infraestructura crítica y servicios esenciales del Estado.3. Proponer acciones eficaces y válidas para la protección y evaluación permanente del nivel de seguridad de los datos en los organismos del Estado.4. Generar política pública de cooperación internacional, con la finalidad de para apoyar y resolver cualquier incidente que tenga lugar dentro del país y pueda ser ocasionado desde el exterior.5. Presentar proyectos de investigación y transferencia tecnológica con la finalidad de identificar, prevenir y compartir información de amenazas y riesgos que podrían provocar incidentes a los componentes de tecnología que procesan, almacenan y transmiten información del Estado.6. Coordinar y cooperar con organizaciones tanto públicas como privadas, para de manera conjunta cumplir la reglamentación correspondiente a los fines de preservar un nivel de Seguridad Digital.7. Las demás atribuciones que las establezca la presente Ley. • Señala que la gestión de vulnerabilidades es una medida de control que se deberá ejecutar por cada una de las instituciones públicas, de manera que

		se evidencie la responsabilidad en el uso de la tecnología, de manera específica de los sistemas y aplicaciones. • Respecto a las funciones del Ministerio de Gobierno, recomienda una nueva: "1. Coordinar con las instituciones públicas, el cumplimiento de las políticas o directivas emitidas por el Sistema Nacional de Seguridad Digital"; y respecto del numeral 2° propone la siguiente función: "2. Coordinar y apoyar en la definición y establecimiento de una metodología de evaluación que permita identificar el nivel de seguridad digital y el cumplimiento de las políticas y otra normativa expedida por el Sistema Nacional de Seguridad Digital, en las instituciones públicas del Estado" • Respecto de las funciones del Ministerio de Telecomunicaciones señala que: "Se debe considerar que el MINTEL es un ejecutor operativo de la propuesta de ley y se debe procurar su aporte desde el punto de visto de proceso de apoyo; otro aporte de tipo estratégico debe ser considerado directamente al rector del ente." • Respecto de las funciones del CIES propone una nueva "1. Coordinar el intercambio de información que permita la toma de decisiones para la mejora continua de la ciberseguridad". • Respecto del Subsistema de Ciberdefensa, propone un texto alternativo: "El subsistema de ciberdefensa estará conformado por: Delegado del Sistema Nacional de Seguridad Digital. Misterio de Defensa. Comando Conjunto de las Fuerzas Armadas y tendrá coordinación directa con el subsistema de ciberinteligencia, quien intercambiará la información necesaria para la protección de la soberanía del estado y la protección de la Infraestructura Crítica y servicios esenciales. En relación a las funciones del subsistema será ciberdefensa además de las apoyar de manera inmediata ante las amenazas, riegos, ataques, y manejo de crisis serán las que señalen en el reglamento de esta Ley". • Respecto de las funciones del Ministerio de Defensa "Se recomienda que las funciones sean sintetizadas y en caso de requerir algo adicional se podría expedir mediante normativa secundaria desde el ente rector" • En relación al Subsistema de Ciberinteligencia señala que su principal función es la identificación y alerta de amenazas, por lo que propone un texto alternativo: 1. Cumplir y hacer cumplir con las políticas públicas, estrategias, planes emitidos por el ente rector de la materia. 2. Coordinar con las instituciones públicas y privadas en el entorno de la seguridad digital, el intercambio de información, referente a amenazas y riesgos. 3. Coordina la cooperación internacional, en materia de intercambio de información con la finalidad de alertar de amenazas que pongan en riesgo la defensa y soberanía del Estado. 4. Recopilar información de incidentes que involucren la Seguridad Digital, y emitir información al subsistema de ciberseguridad para la actualización de políticas y normativa que mejore el entono de la Seguridad Digital. 5. Apoyar en la respuesta a incidentes, mediante su investigación técnica, recopilación de evidencias y otras acciones que aporten a contener un incidente cuando sea requerido por instituciones públicas o privadas. 6. Las demás atribuciones que las establezca el presente reglamento.

		• **Observaciones Proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos [4]** - Propone un nuevo texto para el objeto de la Ley: El objeto de la Ley es garantizar la seguridad y seguridad sistémica del Estado Ecuatoriano en el ciberespacio, proteger la seguridad de las infraestructura crítica y servicios esenciales, establecer el Sistema Nacional de Ciberseguridad, promover la coordinación y articulación institucional e internacional, prevenir, gestionar, investigar y enfrentar amenazas en el ciberespacio, garantizar el acceso a la verdad de los hechos; y, fomentar una cultura de la ciberseguridad. - Se promoverá la asistencia, colaboración y cooperación nacional e internacional para alcanzar la seguridad sistémica, seguridad integral, ciberseguridad y acceso a la verdad de los hechos. - Sobre los operadores de servicios esenciales sugiere "Analizar la definición de las operadoras de servicios esenciales establecidos en el Ecuador". - Respecto del ámbito de aplicación sugiere primero identificar y declarar l infraestructura crítica en lugar de "acreditar". - Respecto del objeto de la Ley, indica que "Uno de los objetivos de protección como bien se indica son las Infraestructuras críticas y los servicios esenciales". - Sobre los operadores de servicios esenciales sugiere "Analizar la definición de las operadoras de servicios esenciales establecidos en el Ecuador". - Respecto del ámbito de aplicación, señala que este componente debe ser parte del Art. 11. - Propone una nueva definición de Ciberinteligencia "Actividades de inteligencia en soporte de la ciberseguridad. Se trazan ciber amenazas, se analizan las intenciones y oportunidades de los ciber adversarios con el fin de identificar, localizar y atribuir fuentes de ciberataques". - Respecto del principio de Seguridad sistémica indica que constituye una definición por lo cual debería ir en la parte correspondiente. - Respecto del Sistema Nacional de Ciberseguridad, "recomienda que se especifique, si las acciones que se desprendan de la presente ley afectarán únicamente al sector público o también a proveedor, e inclusive entidades privadas". - En relación a la conformación del Consejo Nacional de Ciberseguridad, señala que "Es importante como se ha integrado la participación de los delegados de las actividades de seguridad de la información de las entidades públicas, sin embargo, es importante identificar el proceso de selección que los mismos tendrían así como de las entidades privadas". - Respecto de las atribuciones del Consejo Nacional de Ciberseguridad, sugiere "Establecer un metodología, procesos o un mecanismo de evaluación de las medidas de ciberseguridad"; y, además, "Aprobar anualmente el informe de seguimiento sobre ciberataques y ciber amenazas registrarlo en el Sistema Nacional de Ciberseguridad y el estado judicial procesal". - Recomienda realizar un paso adicional y considerar el apoyo del Servicio de Acreditación Ecuatoriano (SAE), para que se defina un marco que

[4] ANEXO 4: Observaciones Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos

		permita un entorno de trabajo, es decir, entidades de certificación y auditores. - Con relación a las certificaciones indica que "Se valora importante el desarrollo del marco de certificación, lo cual a funcionado de manera excelente en otros países"
	Coronel (SP) Fausto Cobo, Director General de Centro de Inteligencia Estratégica Oficio Nro. CIES-CIES-0195-2022-OF [5]	• Presenta una propuesta de unificación de los tres proyectos de ley[6].
	General (SP) Luis Lara Jaramillo Ministro de Defensa Nacional Oficio Nro. MDN-MDN-2022-0982-OF[7]	• **Observaciones Proyecto Ley de Seguridad Digital[8]** - Señala que la ciberdefensa desarrolla operaciones militares en el dominio del ciberespacio y es transversal a los otros dominios, por lo que propone una nueva definición. - Menciona que ciberespacio es un ámbito conceptual intangible, por lo que plantea una nueva definición. - En relación con las funciones del Ministerio de Defensa y Comando Conjunto de las FF.AA. dentro del subsistema de ciberdefensa, señala que la ciberdefensa desarrolla operaciones militares en el dominio del ciberespacio y es transversal a los otros dominios. - Aclara la misión del COCIBER (Comando de Ciberdefensa), en los siguientes términos: "realizar operaciones de defensa, exploración y respuesta en el ciberespacio para proteger la infraestructura crítica digital y servicios esenciales del estado e infraestructura crítica digital de defensa". - Indica que el plan de ciberdefensa debe ser aprobado por el MIDENA y no por el Director Nacional de Seguridad Digital, pues la ciberdefensa es competencia de FFAA y su misión está definida. - Señala que se debe definir el término de Infraestructura Crítica Digital (ICD), para lo cual propone establecer la metodología para la identificación y catalogación de la infraestructura crítica digital del Estado. • **Observaciones Proyecto Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa, Ciberinteligencia.** - Sugiere que se cambien el nombre de la ley, proponiendo "Ley Orgánica de Seguridad Digital", pues esta implica la protección de información y

[5]ANEXO 5: Oficio Nro. CIES-CIES-0195-2022-OF
[6] ANEXO 6: Propuesta de Unificación CIES: Ley de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia
[7] ANEXO 7: Oficio Nro. MDN-MDN-2022-0982-OF
[8] ANEXO 8: Matriz de Observaciones a los Proyectos de Seguridad Digital, MIDENA

		servicios digitales, considerando su organización, estructuración, conservación, adaptación, modificación, extracción, consulta, utilización, etc. - Respecto del objeto de la ley, señala que la resiliencia está orientada a la recuperación de las Infraestructuras Críticas Digitales y sus servicios esenciales. - Indica que el ciberespacio es un ámbito conceptual intangible. - Respecto de los principios indica que el ciberespacio no tiene límites y fronteras, por lo tanto, requiere de alianzas y convenios internacionales para la gestión de los ciberdelitos. - Con respecto al Sistema Nacional de Seguridad Digital, señala que la resiliencia informática es la capacidad de un sistema para recuperarse de un fallo y conservar la confiabilidad del servicio cuando este las presenta, su objetivo es asegurar que todas las operaciones comerciales estén protegidas, para que así una amenaza o incumplimiento no afecte todo el negocio. - Respecto a las funciones y atribuciones del Secretario del Consejo de Seguridad Pública y del Estado, sugiere cambiar el literal 4, relativo a supervisar y monitorear los riesgos y las medidas de ciberseguridad, ciberdefensa y ciberdelitos, para la protección de la infraestructura crítica digital, sugiere aumentar "a través de un Centro de Operaciones de Seguridad (SOC), de las ciber amenazas a las ICD del Estado". • **Observaciones Proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos** - Sugiere que se cambien el nombre de la ley, proponiendo "Ley Orgánica de Seguridad Digital", pues esta implica la protección de información y servicios digitales, considerando su organización, estructuración, conservación, adaptación, modificación, extracción, consulta, utilización, etc. - Sugiere cambiar el nombre Sistema Nacional de Ciberseguridad por Sistema Nacional de Seguridad Digital, con la finalidad de mantener armonía acorde al cambio de denominación de la Ley. - Establecer el término de "Infraestructura Crítica Digital" (ICD) para todo el documento en lugar de "infraestructura crítica y estratégica ubicadas en el territorio nacional". - Señala que el Consejo Nacional de Ciberseguridad como un organismo de alto nivel no tendría como atribución la actualización del catálogo de las ICD. - Sugiere la definición de ICD: "Son aquellas infraestructuras cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales". - Plantea una nueva definición de ciberespacio: "es el entorno conceptual en el que se produce la comunicación a través de redes informáticas". - Plantea una nueva definición de ciberdefensa: "es la capacidad de las Fuerzas Armadas para combatir en el ciberespacio con personal capacitado y entrenado, equipamiento y doctrina, para materializar operaciones militares defensivas, de exploración y respuesta.

		- Plantea una nueva definición de servicio esencial: "El servicio esencial es aquel servicio público que al ser anulado o neutralizado pone en peligro la sobrevivencia de la sociedad o de las organizaciones del Estado". - Respecto de la definición de Sistema Informático señala que un sistema no es un dispositivo aislado, por lo que plantea una definición modificada: "Sistema informático: es un conjunto de dispositivos". - Respecto de los principios de confidencialidad, Disponibilidad e Integridad, sugiere utilizar la definición empleada en la Estrategia Gubernamental de Seguridad de la Información. - Respecto de las Funciones del ente rector de la política pública de defensa, sugiere eliminar el literal relativo a la respuesta a las ciber amenazas y ciberataques mediante acciones técnicas, oportunas y estratégicas, recopilando pruebas o evidencias; y, reporte de los resultados a la Agencia Nacional de Ciberseguridad, indicando que es una situación muy táctica que no debe ser incluida en la ley y; además, sugiere incluir un nuevo numeral: "Fortalecer la Capacidad Estratégica de Ciberdefensa de Fuerzas Armadas". - Respecto de las Funciones del ente rector de la política pública de defensa, sugiere eliminar el literal relativo a gestionar que los recursos humanos y técnicos de las entidades a su cargo se encuentren debidamente capacitados en materia de ciberseguridad, seguridad sistemática y acceso a la verdad de los hechos, debido a que es una situación muy táctica que no debe ser incluida en la ley. - Respecto de las Funciones del ente rector de la política pública de seguridad ciudadana y convivencia social pacífica, sugiere incluir: "Fortalecer la Capacidad Estratégica de Ciberseguridad del Estado"; y, de igual forma, eliminar el numeral relativo a la respuesta a las ciber amenazas y ciberataques mediante acciones tácticas, oportunidad y estratégicas, recopilar pruebas o evidencias; y, reporte de los resultados a la Agencia Nacional de Ciberseguridad, pues se debe considerar al CERT Nacional, que no contempla la propuesta de ley, para la gestión de incidentes de la ICD del Estado y la resiliencia. Adicional es necesario redefinir las funciones del actual EcuCERT, ya que en la propuesta no se considera a este organismo y se traslapan con las funciones de la Agencia Nacional de Ciberseguridad que se propone en el proyecto. - Respecto a las funciones del ente rector de la política pública de telecomunicaciones, sugiere eliminar el literal relativo a la respuesta a las ciber amenazas y ciberataques mediante acciones tácticas, oportunidad y estratégicas, recopilar pruebas o evidencias; y, reporte de los resultados a la Agencia Nacional de Ciberseguridad. - Respecto a las funciones de las y los responsables de ciberseguridad y acceso a la verdad de los hechos de la infraestructura crítica, entidades públicas y privadas sugiere eliminar lo privado debido a que la responsabilidad del Estado es el aparato público. - Sugiere eliminar el artículo relativo a "Ejercicios de vulnerabilidades" pues una situación muy táctica que no debe ser incluida en la ley. - Sugiere incluir como herramienta el concepto de "SOC" o los repositorios de alerta temprana en el ciberespacio.

Elaboración: Comisión Especializada Permanente de Soberanía Integración y Seguridad Integral.[9]

2.3. Detalle de la socialización realizada por la Comisión

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

Tabla 3: Socialización y sesiones de la Comisión

SESIÓN FECHA	PUNTOS TRATADOS
No. 20 06 de agosto de 2021	• Conocer el Proyecto de Ley de Seguridad Digital presentado por el ex Asambleísta Juan Carlos Yar
No. 31 27 de agosto de 2021	• En el marco del tratamiento al Código Orgánico de Seguridad del Estado, a fin de que presenten sus observaciones en la parte correspondiente a seguridad digital, recibir en comisión general a Daniel Tenorio Salazar, experto en ciberseguridad.
No. 38 17 de septiembre de 2021	• .En el marco del tratamiento del "Proyecto de Ley de Código de Seguridad del Estado", recibir en comisión general para que expongan sus observaciones y comentarios, a: -Abogada Alexandra Vela Puga, Ministra de Gobierno o su delegado. -Señor Pablo Jurado, presidente del Consorcio de Gobiernos Autónomos Provinciales del Ecuador CONGOPE. -Señor ingeniero Gabriel Llumiquinga y doctor Santiago Acurio, presidente y vicepresidente, respectivamente, de la Asociación Ecuatoriana de Ciberseguridad.
No. 59 24 de noviembre de 2021	• Avocar conocimiento del "Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia", presentado por el asambleísta Rodrigo Fajardo Campoverde
No. 64 3 de diciembre de 2021	• Recibir en Comisión General al señor doctor Alejandro Padín Vidal quien, como experto en materia de Ciberseguridad, en el marco del tratamiento del proyecto de Código Orgánico de Seguridad del Estado, brindará sus observaciones y recomendaciones sobre el referido proyecto.
No. 98 08 de marzo de 2022	• Avocar conocimiento del Proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos, presentado por el señor asambleísta José Luis Vallejo Ayala.

[9] Para más información de las observaciones y aportes ciudadanos, se puede consultar en el anexo 1, la sistematización íntegra de las observaciones recibidas por escrito.

No. 107 30 de marzo del 2022	• Conocer las motivaciones y argumentaciones del "Proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos", a cargo del señor asambleísta José Luis Vallejo Ayala, PhD.
No. 109 06 de abril del 2022	• Conocer y Resolver sobre la propuesta de unificación del Proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos al Proyecto de Código Orgánico de Seguridad Integral
No. 132 15 de junio de 2022	• En el marco del tratamiento de los proyectos de ley sobre ciberseguridad presentados por los señores asambleístas Juan Carlos Yar Araujo, Rodrigo Olmedo Fajardo Campoverde y José Luis Vallejo Ayala, recibir en Comisión General a las siguientes autoridades: a. Señor General de División (S.P.) Luis Eduardo Lara Jaramillo, Ministro de Defensa Nacional o su delegado; b. Señor magíster Juan Carlos Holguín Maldonado, Ministro de Relaciones Exteriores o su delegado; c. Señor General Inspector (S.P.) Hernán Patricio Carrillo Rosero, Ministro del Interior o su delegado; d. Señor Coronel E.M. (S.P.) Fausto Antonio Cobo Montalvo, Director General del Centro de Inteligencia Estratégica o su delegado; y, e. Señora doctora Vianna Di María Maino Isaías, Ministra de Telecomunicaciones y Sociedad de la Información.
No. 133 15 de junio del 2022	• En el marco del tratamiento de los proyectos de ley sobre ciberseguridad presentados por los señores asambleístas Juan Carlos Yar Araujo, Rodrigo Olmedo Fajardo Campoverde y José Luis Vallejo Ayala, recibir en Comisión General a los siguientes expertos: 1. Señora abogada María Alexandra Maldonado Navarro, magíster en Derecho Público; y, 2. Señor abogado Luis Fernando Enríquez Álvarez, Master of Laws y magíster en Derecho Mención Derecho Internacional Económico, miembro del Observatorio de Ciberderechos de la Universidad Andina Simón Bolívar.
No. 157 24 de agosto de 2022	• Recibir en Comisión General al señor abogado Diego Álvarez, asesor en materia de política pública Amazon Web Services AWS, quien se referirá respecto a las iniciativas legislativas sobre ciberseguridad que se tramitan en la Comisión, con miras a buscar la transformación digital del país y que mejoren la protección de la información en el ciberespacio.
No. 160 31 de agosto de 2022	• Con la finalidad de recibir sus observaciones y recomendaciones los proyectos de ley sobre ciberseguridad presentados por el ex asambleísta Juan Carlos Yar y los asambleístas Rodrigo Fajardo Campoverde y José Luis Vallejo, recibir al señor doctor Juan Carlos Soria Cabrera, Director Ejecutivo encargado de la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL.
No. 162 7 de septiembre de 2022	• En el marco del tratamiento de los proyectos de Ley de Seguridad Digital, Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia y Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos presentados por el ex legislador Juan Carlos Yar, y los legisladores Rodrigo Fajardo Olmedo y José Luis Vallejo, respectivamente, recibir en comisión general para que exponga sus observaciones y análisis a:

	Magíster Jonathan Marcelo Ramos Mera, Catedrático de Derechos Penal de la Universidad Central del Ecuador y Representante de la Asociación Académica Ecuatoriana de Derecho e Informática.
No. 164 9 de septiembre de 2022	• 1. En el marco del tratamiento a los proyectos de Ley de Seguridad Digital, Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia y Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos presentados por el ex legislador Juan Carlos Yar y los legisladores Rodrigo Fajardo Olmedo y José Luis Vallejo, respectivamente, recibir en comisión general para que exponga sus observaciones y criterios, a: Fausto Antonio Cobo Montalvo, Director General del Centro de Inteligencia Estratégica.
Nro. 209 23 de febrero del 2023	• Punto Único: Revisión y debate de los textos del Proyecto de Ley Orgánica de Seguridad Digital.
No. 211 24 de febrero del 2023	• Punto Único: Continuación de la revisión y debate de los textos del Proyecto de Ley Orgánica de Seguridad Digital.

Elaboración: Comisión Especializada Permanente de Soberanía Integración y Seguridad Integral.

2.4. Asistencias de las legisladoras y legisladores de la Comisión

A continuación, se agregan las asistencias de las y los señores legisladores, durante el proceso de socialización y tratamiento del Informe para Primer Debate del Proyecto de Ley.

Tabla 4: Asistencia de las legisladoras y legisladores agosto 2021-junio 2022

CONVOCATORIA	**20**	**31**	**38**	**59**	**64**	**98**	**107**	**109**	**132**	**133**	**TOTAL ASISTENCIAS**
MES:	**Agosto 2021**		**Septiembre 2021**	**Noviembre 2021**	**Diciembre 2021**	**Marzo 2022**		**Abril 2022**	**Junio 2022**		
Asambleísta/ FECHA	06	27	17	24	3	8	30	06	15	15	
María Aquino	P	P	P	P	P	P	P	P	P	P	Asistencias: 10 Alterno: Ausencias:
Rodrigo Fajardo	P	P	P	P	P	P	P	P	P	P	Asistencias: 10 Alterno: Ausencias:

Augusto Guamán	P	P	P	P	P	P	P	P	P	P	Asistencias: 10 Alterno: Ausencias:
Xavier Jurado	X*	P	P	X**	P	P	P	P	P	P	Asistencias: 8 Alterno: Ausencias: 2
Patricia Núñez	P	P	P	P	P	P	P	P	P	P	Asistencias: 10 Alterno: Ausencias:
Jorge Pinto	P	P	P	P	P	P	X	P	P	P	Asistencias: 9 Alterno: Ausencias: 1
José Luis Vallejo	P	P	P	P	P	P	P	P	P	P	Asistencias: 10 Alterno: Ausencias:
Geraldine Weber	P	P	P	P	P	P	P	P	P	P	Asistencias: 10 Alterno: Ausencias:
Ramiro Narváez	P	P	P	P	P	P	P	P	P	P	Asistencias: 10 Alterno: Ausencias:

Nota*: El señor asambleísta Jurado justifica su inasistencia mediante memorando AN-JBXA-2021-0043 M de fecha 10 de agosto de 2021.

Nota:** El señor Asambleísta Xavier Jurado justifica su inasistencia mediante Memorando Nro. AN-JBXA-2021-0092-M de 26 de noviembre de 2021 al que adjunta el respectivo certificado médico.

Elaboración: Comisión Especializada Permanente de Soberanía Integración y Seguridad Integral.

Tabla 5: Asistencia de las legisladoras y legisladores julio 2022-marzo 2023

CONVOCATORIA	**157**	**160**	**162**	**164**	**209**	**211**	**219**	**TOTAL ASISTENCIAS**
MES:	**Agosto 2022**		**Septiembre 2022**		**Febrero 2023**		**Marzo 2023**	
Asambleísta/ FECHA	24	31	07	09	23	24	22	

María Aquino	P	P	P	P	N/A	N/A	N/A	Asistencias: 4 Alterno:0 Ausencias: 0
Simón Remache[10]	N/A	N/A	N/A	N/A	P	P	P	Asistencias: 3 Alterno: 0 Ausencias:0
Rodrigo Fajardo	P	P	X	X	P	P	P	Asistencias: 5 Alterno:2 Ausencias: 0
Gissela Castillo*	N/A	N/A	P	P	N/A	N/A	N/A	Asistencias: 2
Augusto Guamán	P	P	P	P	P	P		Asistencias: 6 Alterno:1 Ausencias:0
Stalin Ballas	N/A	N/A	N/A	N/A	N/A	N/A	P	Asistencias: 1
Xavier Jurado	X	X	P	P	P	P		Asistencias: 4 Alterno:2 Ausencias: 1
Eleana Romero**	P	P	N/A	N/A	N/A	N/A	N/A	Asistencias: 2
Patricia Núñez	P	P	P	P	P	P	P	Asistencias: 7 Alterno: 0 Ausencias:0
Jorge Pinto	X	P	X	P	P	P	P	Asistencias: 5 Alterno:2 Ausencias:
María Belén Álvarez***	P	N/A	X	N/A	N/A	N/A	N/A	Asistencias: 1 Ausencias: 1
José Luis Vallejo	P	P	X	X	P	P	P	Asistencias: 5 Alterno:2 Ausencias: 0
Yolanda Obando	N/A	N/A	P	P	N/A	N/A	N/A	Asistencias: 2
Geraldine Weber	P	X	P	P	X	X	P	Asistencias: 4 Alterno:3 Ausencias:

[10] El asambleísta Simón Bolívar Remache era alterno de la Asambleísta María Aquino y la reemplazó cuando esta presento su renuncia a su curul en la Asamblea Nacional.

Gustavo Loor****	N/A	P	N/A	N/A	P	P	N/A	Asistencias: 3
Ramiro Narváez	P	P	P	P	X	X	P	Asistencias: 5 Alterno:2 Ausencias: 0
Mónica Ati**	N/A	N/A	N/A	N/A	P	P	N/A	Asistencias: 2

NOTA*: La Asambleísta Gissela Castillo es alterna del Asambleísta Rodrigo Fajardo y fue posesionada mediante Memorando Nro. AN-FCRO-2022-0071-M,

NOTA:** La Asambleísta Eleana Romero es alterna del Asambleísta Xavier Jurado y fue posesionada mediante Memorando Nro. AN-JBXA-2022-0105-M, comunicado a esta secretaría mediante Memorando Nro. AN-RREM-2022-0006-M.

NOTA*:** La Asambleísta María Belén Álvarez es alterna del Asambleísta Jorge Pinto y fue posesionada mediante Memorando Nro. AN-PDJW-2022-0084-M.

NOTA**:** El Asambleísta Gustavo Loor es alterno de la Asambleísta Geraldine Weber y fue posesionado mediante Memorando Nro. AN-WMG-2022-0054-M, mismo que modificó al Memorando Nro. AN-WMG-2022-0053-M.

3. BASE CONSTITUCIONAL, LEGAL E INTERNACIONAL PARA EL TRATAMIENTO DEL PROYECTO DE LEY

3.1 Constitución de la República del Ecuador

El numeral 3 del artículo 120 de la Constitución de la República, determina que la Asamblea Nacional tiene las siguientes atribuciones y deberes: *(...) "3. Expedir, codificar, reformar y derogar las leyes, e interpretarlas con carácter generalmente obligatorio".*

El artículo 136 de la Norma Suprema al referirse a los requisitos de los proyectos de ley, determina:

> 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. (Negritas agregadas)

En relación con el procedimiento parlamentario, la Constitución establece en el artículo 137:

> 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. (…)

3.2 Ley Orgánica de la Función Legislativa

La Ley Orgánica de la Función Legislativa señala:

> Art. 57.- Tratamiento del proyecto de ley.- Recibido el proyecto de ley calificado por el Consejo de Administración Legislativa, la Presidenta o el Presidente de la comisión especializada dispondrá a la Secretaria o al Secretario Relator, informe su recepción a las y los integrantes de la comisión y convoque para su conocimiento e inicio de su tratamiento.

> Avocado conocimiento del proyecto de ley, la Presidenta o el Presidente de la comisión dispondrá se informe del inicio del tratamiento y apertura de la fase de socialización a las y los demás legisladores de la Asamblea Nacional y a la ciudadanía, a través del portal web y demás canales comunicacionales que disponga la Asamblea Nacional y la comisión.
>
> Art. 60.- Inclusión del informe para primer debate en el orden del día.- El primer debate se desarrollará, previa convocatoria del Presidente o de la Presidenta de la Asamblea Nacional, en una sola sesión en un plazo máximo de sesenta días de remitido el informe por la comisión. **Las y los asambleístas presentarán sus observaciones por escrito en el transcurso de la misma sesión o hasta treinta días después de concluida la sesión.** (Negritas añadidas)

3.3 Reglamento de las Comisiones Especializadas Permanentes y Ocasionales

El artículo 8, numero 8, del Reglamento de las Comisiones Especializadas Permanentes y Ocasionales, establece que son funciones del Pleno de las comisiones:

> 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.
>
> Los informes de los proyectos de ley serán aprobados por las comisiones especializadas permanentes y ocasionales y, contendrán los parámetros mínimos definidos como formato en el artículo 30 del referido Reglamento.

4. PLAZO PARA EL TRATAMIENTO DEL PROYECTO DE LEY

El artículo 58 de la Ley Orgánica de la Función Legislativa, determina:

> Art. 58.- Informes para primer debate.- Las comisiones especializadas, **dentro del plazo máximo de noventa días contados a partir de la fecha de inicio del tratamiento del proyecto de ley**, presentarán a la Presidenta o al Presidente de la Asamblea Nacional su informe con las observaciones que juzguen necesarias introducir. Dentro del referido plazo, se considerará un tiempo no menor a los quince primeros días, para que 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, acudan ante la comisión especializada y expongan sus argumentos. En ningún caso, la comisión especializada emitirá su informe en un plazo menor a veinte días. (…) (Negritas añadidas)

Por lo expuesto, las comisiones especializadas permanentes u ocasionales tienen la obligación de presentar el Informe para primer debate en el plazo de 90 días desde el inicio del tratamiento del Proyecto de ley, no obstante, la norma permite solicitar una prórroga debidamente justificada.

El Presidente de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, mediante Memorando Nro. AN-CSIS-2022-0377-M de 08 de junio de 2022, solicitó *"se sirva conceder una prórroga de 90 días para la presentación del Informe para Primer Debate del "Proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos",*

presentado por el señor asambleísta José Luis Vallejo Ayala, Ph.D. Este pedido lo realizo por cuanto el proyecto, dada la novedad y complejidad técnica de la temática, requiere un mayor tiempo para su debido procesamiento".

Mediante Memorando Nro. AN-SG-2022-2327-M de 02 de julio de 2022, el Secretario General de la Asamblea Nacional, Abg. Álvaro Salazar Paredes, informó que en atención a lo establecido en el segundo inciso del artículo 58 de la Ley Orgánica de la Función Legislativa, se ha autorizado una prórroga para la presentación del referido Informe para Primer Debate por noventa (90) días.

5. ANÁLISIS Y RAZONAMIENTO REALIZADO POR LOS MIEMBROS DE LA COMISIÓN EN LA ELABORACIÓN DEL INFORME PARA PRIMER DEBATE

5.1. Estándares y organizaciones internacionales en materia de seguridad digital

La seguridad digital se ha convertido en un tema de importancia mundial, ya que la conectividad en línea ha aumentado significativamente y con ella, también la cantidad de amenazas cibernéticas. Para garantizar una seguridad adecuada en el mundo digital, existen estándares internacionales que se han establecido para orientar a las organizaciones, gobiernos y ciudadanos en la implementación de medidas efectivas para protegerse de las amenazas cibernéticas.

Uno de los estándares más importantes en este campo es el conjunto de normas ISO/IEC 27001 y 27002. Estas normas establecen los requisitos y directrices para la gestión de la seguridad de la información. La ISO/IEC 27001 proporciona una guía para la implementación de un sistema de gestión de la seguridad de la información en una organización, mientras que la ISO/IEC 27002 proporciona una lista de controles de seguridad que pueden implementarse para reducir los riesgos a la seguridad de la información. La adopción de estos estándares puede ayudar a una organización a identificar y protegerse contra posibles amenazas a la seguridad de la información, y a garantizar la confidencialidad, integridad y disponibilidad de los datos.

Otro estándar importante en el campo de la seguridad digital es el NIST Cybersecurity Framework, desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos. Este marco proporciona orientación para la gestión de riesgos de seguridad cibernética a nivel organizacional, con el objetivo de ayudar a las organizaciones a protegerse contra posibles amenazas a la seguridad de la información.

En el ámbito de la seguridad cibernética, también existen estándares internacionales como el Marco Nacional de Ciberseguridad de los Estados Unidos, que establece un conjunto de principios y prácticas para garantizar la seguridad digital en el país. Este marco se basa en las mejores prácticas y estándares existentes y ha sido adoptado por muchas empresas y organizaciones en todo el mundo.

Otro estándar importante en la seguridad cibernética es el CIS Controls, desarrollado por el Centro de Seguridad Cibernética (CIS) en Estados Unidos. Estos controles establecen un conjunto de

prácticas para garantizar la seguridad de los sistemas informáticos, y han sido adoptados por muchas organizaciones en todo el mundo.

Ahora bien, a nivel convencional, la seguridad digital no tiene un marco de regulación único, al contario, existe una pluralidad de normas de mayor o menor complejidad técnica, a las que se suman una serie de instrumentos de *soft law* como resoluciones, pronunciamientos, principios o recomendaciones no vinculantes, pero altamente útiles y aplicables.

No obstante, se pude destacar el grado de evolución del marco normativo de la Unión Europea, que cuenta, entre otras normas, con el Reglamento 2019/881 de 17 de abril de 2019 relativo a la Agencia de la Unión Europea para la Ciberseguridad y a la certificación de la ciberseguridad de las tecnologías de la información y comunicación.

Este reglamento establece como objeto en su artículo 1:

"Con vistas a garantizar el correcto funcionamiento del mercado interior, aspirando al mismo tiempo a alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión, el presente Reglamento establece:

a) los objetivos, tareas y aspectos organizativos relativos a ENISA (Agencia de la Unión Europea para la Ciberseguridad), y

b) un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad en la Unión. (…)".

Así mismo, en lo relativo a la ciberdelincuencia, se destacada el Convenio sobre la Ciberdelincuencia, conocido como "Convenio de Budapest", el cual establece que los estados partes deben adoptar una serie de medidas legislativas y de otro tipo para tipificar delitos como el acceso ilegítimo a un sistema informático; la interceptación ilegítima de datos informáticos no públicos; actos deliberados que borren, deterioren, alteren o supriman datos informáticos; la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático; la falsificación informática; el fraude informático; delitos relacionados con la pornografía infantil; delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, entre otros.

Si bien este Convenio emerge en el marco de la Unión Europea, está abierto a la firma de otros estados que hayan sido invitados a ser parte de este y cumplan los requisitos técnicos para este propósito[11].

[11] El art. 37 de Convenio de Budaspest establece que: "A partir de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá, previa consulta con los Estados contratantes del Convenio y habiendo obtenido su consentimiento unánime, invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo de Europa y que no haya participado en su elaboración. La decisión se adoptará respetando la mayoría establecida en el artículo 20.d del Estatuto del Consejo de Europa y con el voto unánime de los representantes de los Estados contratantes con derecho a formar parte del Comité de Ministros. (…)"

La cooperación a nivel internacional se desarrolla a través de organizaciones privadas o iniciativas técnicas de cooperación. Por ejemplo, la agrupación de los Centros de Respuesta a Incidentes Informáticos (CERT) se realiza bajo el paraguas de la organización *FIRST* que es el Foro de Equipos de Seguridad y Respuesta a Incidentes, creado en 1989, y que su vez otorga las acreditaciones a las entidades que deseen ser reconocidas como parte de esta red.

Otra de las comunidades de cooperación que existen a nivel internacional es el *Trusted Introducer* TF-CSIRT[12], conformado por una red de equipos de seguridad y respuesta ante incidentes informáticos en todo el mundo, establecido en el año 2000 con el objetivo de ayudar a mejorar la cooperación colectiva e incrementar la seguridad gracias a respuestas más ágiles frente a los ataques o amenazas existentes o nuevas.[13]

De igual manera, a nivel internacional, existe un marco referencial que sirve de orientación para que los países puedan desarrollar su normativa local.

De su parte, la Unión Internacional de las Telecomunicaciones ha creado una "*Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad",* que sirve de referente para el desarrollo de este tipo de herramienta a nivel local.

En el ámbito de la formación y capacitación, se realizan ejercicios de simulación o programas de formación a todo nivel, como por ejemplo el *Cybersecurity Summer BootCamp* organizado por el Instituto Nacional de Ciberseguridad de España, que agrupa a delegados de todos los países Latinoamericanos y otras regiones del mundo.

Son muchos los espacios de coordinación en favor de la ciberseguridad con los que se cuenta a nivel nacional e internacional en los cuales se pueden encontrar redes de cooperación a distintos niveles, desde el intercambio de información clasificada entre Estados en el marco de una investigación legal, hasta la asistencia técnica mutua o la formación en la materia.

Esta situación responde a que la seguridad digital se caracteriza por una realidad convergente en la que los estados y sociedades buscan seguridad y certeza en sus comunicaciones e intercambio de información, por lo que los marcos de cooperación requieren ser más amplios, a fin de dar respuesta al problema desde sus múltiples aristas e integrando a todos los actores interesados.

Ahora bien, estos procesos de intercambio son posibles en la medida que las legislaciones nacionales se adaptan a los estándares internacional en aspectos sustantivos y adjetivos, razón por la cual se hace necesario que el Ecuador modifique la legislación que permita a su marco institucional requerir apoyo y contribuir a enfrentar los desafíos del desarrollo de las modernas y emergentes tecnologías.

5.2. Orientaciones en materia de seguridad digital para los parlamentos del mundo

[12] CSIRT por las siglas de Computer Security Incident Response Team)
[13] Información disponible en: Trusted Introducer : Services: Overview of TI Services: TI Overview: Spanish (trusted-introducer.org)

La necesidad de contribuir a la seguridad digital desde el quehacer de los parlamentos ha sido puesta en evidencia por la Unión Interparlamentaria Mundial UIP. Es en este marco y con la colaboración de parlamentarios de 16 países, expertos, académicos y oficiales de gobierno, que se elaboraron en el 2021 los "Los 10 Principios Rectores para la Ciberseguridad Ciudadana."

Este instrumento tiene como principal objetivo, dotar a las y los parlamentarios, sus equipos de técnicos de una herramienta coherente y estructurada, que les permita:

> *(i) Identificar cuáles son aquellos derechos esenciales que todo ciudadano debe tener en un entorno digital;*
>
> *(ii) Incorporar acciones y/o medidas que protejan a las personas de las graves amenazas y efectos dañinos que existen en el ciberespacio; y*
>
> *(iii) Alentar la inclusión, alfabetización y educación digital.*

Conforme se ha señalado por la UIP, los principios rectores de la ciberseguridad ciudadana también buscan que los parlamentos alcancen la necesaria convergencia y confianza digital que les permita innovar en sus esfuerzos para garantizar el ejercicio de una ciudadanía digital plena.

Esto principios son el resultado de un esfuerzo entre legisladoras y legisladores, asesores parlamentarios, expertos del sector privado en los campos de la ciberseguridad y la transformación digital, así como, de académicos y líderes de sociedad civil.

La principal finalidad de estos principios rectores es dotar de una herramienta coherente, rigurosa y estructurada, que les permita a los Estados garantizar una eficaz inclusión, alfabetización y universalización digital. Buscan, además, la creación de políticas públicas, legislaciones, marcos normativos y reglamentos que le ofrezcan a las y los ciudadanos una mejor protección en su interacción con las actuales infraestructuras tecnológicas, como son la Internet, las redes sociales y los sistemas y/o plataformas de la información y de la comunicación.

Los 10 principios rectores de la Ciberseguridad Ciudadana son:

1. Resguardar los derechos y libertades individuales;
2. Preservar la soberanía en la democracia digital;
3. Consagrar la libertad de expresión y la privacidad por defecto en el ciberespacio;
4. Impulsar una cultura de la ciberseguridad;
5. Construir un entorno ciberseguro;
6. Asegurar la privacidad de los datos;
7. Establecer la responsabilidad compartida;
8. Fortalecer el desarrollo de aptitudes y habilidades;
9. Incorporar la educación para la vida en ciberespacio;
10. Involucrar a la ciudadanía en los procesos de creación de marcos normativos que impulsen la innovación y la transformación digital.

La Comisión de Soberanía, Integración y Seguridad Integral ha tomado nota de estos principios

rectores y, en particular de los principios 2, 3, 4, 5, 8 y 10, los mismos que han sido considerados como guías orientadoras en el proceso de construcción normativa que se propone.

5.3. Estado de la Ciberseguridad en la región y en el Ecuador

La seguridad digital es un tema de creciente importancia en todo el mundo y América Latina no es la excepción. Según datos de la Comisión Económica para América Latina y el Caribe (CEPAL), se estima que el costo de los ciberataques en la región superó los 90 mil millones de dólares en 2020. Esta cifra representa un aumento del 400% en comparación con el año 2016 y pone en evidencia la necesidad de contar con políticas y medidas efectivas para abordar esta problemática.

Latinoamérica actualmente tiene una expansión del mercado de comercio en línea conocida como economía digital de más de 53.2 billones de dólares, así como ha invertido más de 100 billones de dólares en infraestructura de ciudades inteligentes, siendo una región que cuenta con más de 385 millones de usuarios de Internet.

Pero, al mismo tiempo, es una región donde es indispensable atender la inmensa brecha digital, procurando mayores y mejores políticas públicas y marcos normativos que permitan la alfabetización y universalización digital, y particularmente, avanzar en promover y garantizar una mayor seguridad informática.[14]

En el caso específico de Ecuador, según el Índice Global de Ciberseguridad 2020, elaborado por la Unión Internacional de Telecomunicaciones (UIT), el país ocupa el puesto 100 a nivel mundial en cuanto a ciberseguridad, con una puntuación de 0.51 en una escala de 0 a 1. Si bien esta puntuación representa una mejora con respecto a años anteriores, aún queda mucho por hacer para fortalecer la seguridad digital en el país.

En Ecuador, la principal amenaza cibernética son los ataques de phishing, que representan el 60% de los incidentes reportados según la Encuesta Nacional de Seguridad Informática realizada en 2020. Los ciberataques también son una amenaza para la infraestructura crítica del país, como los sistemas de energía y los sistemas financieros.

A nivel regional, Brasil es el país más afectado por los ciberataques, seguido de México y Colombia, según un informe de la empresa de ciberseguridad Kaspersky. Además, la región también enfrenta amenazas como el malware, los ataques a la nube, el robo de datos y los ataques a dispositivos móviles.

A pesar de estas amenazas, la inversión en seguridad digital en la región es baja en comparación con otras partes del mundo. Según datos de la UIT, en 2019, América Latina y el Caribe invirtieron

[14] Documento UIP: Mesa de Trabajo acerca de Los 10 principios rectores de la ciberseguridad ciudadana para los poderes legislativos y su posible conexión con el proyecto de resolución de la UIP acerca de "Los ciberataques y los ciberdelitos: los nuevos riesgos para la seguridad mundial".

solo el 0.5% de su PIB en ciberseguridad, en comparación con el 0.8% de Europa y el 0.9% de América del Norte.

Para abordar esta problemática, es necesario fortalecer la cooperación regional en materia de ciberseguridad y aumentar la inversión en tecnología y capacitación en seguridad digital. Además, es fundamental que los gobiernos adopten medidas concretas para promover la seguridad digital, como la creación de marcos regulatorios y la promoción de la educación y concientización sobre seguridad digital.

La Comisión considera que la seguridad digital es una problemática creciente en América Latina y Ecuador. Los ciberataques representan una amenaza para las empresas y la infraestructura crítica en la región. Para abordar esta problemática, es necesario fortalecer la cooperación regional y aumentar la inversión en tecnología y capacitación en seguridad digital. Además, es fundamental que el gobierno adopte medidas concretas para promover la seguridad digital y proteger a los ciudadanos y empresas de la región. Por lo señalado, la presente Ley, se puede constituir en una herramienta fundamental para fortalecer la institucionalidad estatal para la seguridad digital.

El Ecuador es uno de los países de la región con menor nivel de maduración en materia de seguridad digital. Mientras que otros países como Uruguay ya se han sumado al escudo de protección de datos de la Unión Europea, por sus capacidades instadas en ciberseguridad, Ecuador todavía no cuenta con un CERT nacional público, certificado internacionalmente.

El índice mundial de Ciberseguridad, de la Unión Internacional de las Telecomunicaciones que, entre otras cuestiones, evalúa el marco jurídico en materia de seguridad digital, ubica al Ecuador en el puesto 119 de 182 países.[15]

Para tener una referencia de los países de la región, Brasil ocupa el lugar 18, México el 52, Uruguay el 64, Chile el 74, Costa Rica 76, Colombia 81, Cuba 82 y Perú 86. De hecho, en Sudamérica, Ecuador solo supera al Estado Plurinacional de Bolivia que está en el puesto 140.

Esto da cuenta de las limitada capacidades del país, que solo recientemente ha aprobado una Estrategia Nacional de Ciberseguridad, conforme lo requieren los estándares internacionales.

5.4. Pertinencia de un marco legal en materia de Seguridad Digital

La irrupción de tecnologías emergentes, sumado al aparecimiento de COVID-19 y sus medidas de distanciamiento, educación on line, compras virtuales y el desarrollo del teletrabajo han profundizado el proceso de *transformación digital* en la sociedad, tanto a nivel nacional como a nivel regional y global.

El ciberespacio ha creado un verdadero *ecosistema digital* basado en un nuevo paradigma de interconexión que ha cambiado la manera como nos relacionamos entre los seres humanos, eliminando barreras como la distancia, la capacidad de almacenar información o, incluso, la necesidad de contar con espacios físicos para poder reunirnos e interactuar con los demás. Al mismo

[15] Disponible en: Índice Mundial de Ciberseguridad 2020 (itu.int)

tiempo, esta situación ha generado mayor dependencia hacia la tecnología, incrementando las vulnerabilidades y amenazas, que cada vez reportan mayor complejidad, diversidad y dificultad de detección.

La digitalización de la sociedad ha transformado los modelos de relacionamiento e intercambio de información tradicionales, pero también ello implica un riesgo. El aumento de la dependencia de la tecnología incrementa el nivel de exposición de las empresas, entidades públicas y del público en general, multiplicando los vectores de ataque e incrementando la cantidad e impacto de incidentes, ataques o crisis cibernéticas.

Un informe estadístico de la Unidad de Ciberdelitos de la Policía Nacional señala que desde 2020 hasta julio de 2022 se registraron 3183 delitos informáticos. En 2020 se reportaron 682 casos, en 2021 se reportaron 1851 y en 6 meses de 2022 se reportaron 650. Esta tendencia al incremento se correlaciona con el aumento en el uso de internet que, tras la pandemia, llegó al 79,21% de hogares aumentando así el número de transacciones digitales como compra de alimentos u otros bienes, pagos y en general transacciones financieras[16].

De esta manera, se colige que el sector de seguridad digital está en un proceso de expansión, amplificada por efecto de la dinámica de la globalización, las nuevas tecnologías emergentes y la consecuente transformación digital. La irrupción del *internet de las cosas* irá reemplazando los actuales dispositivos por artefactos 100% conectados a la *nube* a través de redes g5. Toda la data generada solo podrá ser almacenada en computadoras *cuánticas* y analizada por *inteligencia artificial* para profundizar el uso del ciberespacio.

El Informe de Percepción de Riesgos Globales 2021 del International Science Council identifica como los principales riesgos tecnológicos la desigualdad digital, la concentración de poder e infraestructura digital, el fracaso de la gobernanza tecnológica, entre otros[17]. El quedarse fuera del proceso de transformación digital es parte de estos riesgos, reducir la vulnerabilidad implica generar un ambiente de confianza y seguridad en las nuevas tecnologías de la información y comunicación.

Es necesario entonces que el Estado no deslinde su rol de regulación, para impulsar este importante sector en su dimensión no solo técnica, sino además económica, pues el país cuenta con el talento humano capacitado y parte de la red de infraestructura necesaria para este fin, pero hace falta la decisión política de todos los niveles de gobierno para dar el apoyo, incluyendo el presupuestario, al desarrollo de la ciberseguridad en el Ecuador.

En la actualidad, el país no cuenta con una ley de seguridad digital, lo que ha provocado una serie de problemas prácticos desde la imposibilidad de los entes estatales de articular una respuesta coordinada, por ejemplo, para adquirir tecnología de seguridad que sean compatible entre las diversas instituciones, contar con un centro de respuesta a incidentes o determinar claramente cuál es el organismo rector encargado de emitir la política pública oficial en la materia.

[16] El Comercio; 3183 delitos informáticos se han registrado en el Ecuador, desde el 2020, 25 de julio de 2022. Disponible en: 3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020 - El Comercio
[17] Disponible en: Informe-de-Percepción-de-Riesgos-Globales-2021.pdf (futureearth.org)

Por lo expuesto, dado el auge que experimenta el sector de la seguridad digital, las modernas manifestaciones de la ciberdelincuencia, la necesidad de determinar un organismo rector y desarrollar las competencias y destrezas necesarias para la seguridad integral del país, la Comisión considera necesario y pertinente contar con una nueva legislación en materia de seguridad digital, por lo cual en el presente informe se propone un nuevo e integral marco legal de regulación.

5.5. Carácter orgánico del proyecto de Ley

La Constitución de la República del Ecuador establece que las leyes orgánicas son jerárquicamente superiores a las leyes ordinarias, estableciendo, además, en el artículo 133 las materias específicas que tienen reserva de ley orgánica, a saber

> Art. 133.- Las leyes serán orgánicas y ordinarias.
>
> Serán leyes orgánicas:
> 1. Las que regulen la **organización y funcionamiento de las instituciones** creadas por la Constitución.
> 2. Las que regulen el ejercicio de los derechos y garantías constitucionales.
>
> (...)
> La expedición, reforma, derogación e interpretación con carácter generalmente obligatorio de las leyes orgánicas requerirán mayoría absoluta de los miembros de la Asamblea Nacional. Las demás serán leyes ordinarias, que no podrán modificar ni prevalecer sobre una ley orgánica. (El resaltado nos corresponde).

Por su parte del artículo 53 de la Ley Orgánica de la Función Legislativa, concordante con la Constitución, se colige que el legislador debe determinar el carácter orgánico u ordinario de una ley, para lo cual ha de tomar en cuenta el ámbito de aplicación de la misma y el objeto sobre el que recae.

En el caso *sub iudice* la Ley Orgánica de Seguridad Digital tiene por objeto restablecer regulaciones para hacer frente a las amenazas, riesgos e incidentes en el ciberespacio u otros entornos digitales, mediante el Sistema Nacional de Seguridad Digital y sus subsistemas.

Entre estos subsistemas se encuentran dos, ciberseguridad y ciberdefensa, que regulan atribuciones de las instituciones reconocidas en la sección tercera "Fuerzas Armadas y Policía Nacional", del capítulo tercero "Función Ejecutiva", del "Título IV Participación Y Organización Del Poder" de la Constitución de la República.

Además, la Ley incluye un enfoque de derechos digitales en su artículo 18, numeral 17 y establece como obligación del Comité Nacional de Seguridad Digital: *"Proponer medidas y estrategias que en el ámbito de la seguridad digital permitan garantizar los derechos digitales y el acceso a la verdad de los hechos".*

Este concepto, entendido como parte de los derechos digitales, el derecho a acceder a la verdad de los hechos, es uno de los enfoques transversales que está regulado en el artículo 75 de forma específica, pero atraviesa todo el proyecto de ley.

La Constitución de la República establece en su artículo 334 que:

El Estado promoverá el acceso equitativo a los factores de producción, para lo cual le corresponderá: (…) 3. Impulsar y apoyar el desarrollo y la difusión de conocimientos y tecnologías orientados a los procesos de producción.

Además, la Norma Suprema, en su artículo 340 crea el sistema nacional de inclusión y equidad social que cuenta entre otros ámbitos con el *tecnológico*, al mismo tiempo que establece como responsabilidad del Estado, en el artículo 347:

> (…) 7.Erradicar el analfabetismo puro, funcional y digital, y apoyar los procesos de post-alfabetización y educación permanente para personas adultas, y la superación del rezago educativo.
> 8. Incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales.

En virtud que el presente Proyecto de ley, incorpora disposiciones que regulan el funcionamiento de la Policía Nacional y las Fuerzas Armadas y que, además, regulan el ejercicio de derechos constitucionales, reconocidos a través de las obligaciones del Estado en la materia, la Comisión conviene en la naturaleza orgánica del Proyecto.

5.6. Principales aspectos debatidos en la Comisión

5.6.1. Objeto de la Ley y Ámbito de Aplicación

La Comisión, a través de las mesas técnicas en las que participaron los legisladores, sus equipos de asesores y las instituciones invitadas, debatieron intensamente en torno a objeto del proyecto de ley y su ámbito de aplicación, sobre todo en lo relacionado con la regulación de los "derechos digitales".

En este sentido, el Parlamento Europeo ha reconocido que los sistemas de información, las redes y servicios de comunicaciones electrónicas, se han convertido en la espina dorsal del crecimiento económico, puesto que las Tecnologías de la Información y Comunicación (TIC) son la base de los sistemas que sustentan las actividades cotidianas de la sociedad y garantizan el funcionamiento de nuestras economías.

Por tanto, se acordó que esta ley debía tener dentro de su objeto el normar los mecanismos y herramientas institucionales para promover la seguridad del Estado, la confianza digital, la cultura de seguridad en el ciberespacio y la protección de derechos humanos.

De esta manera, se reconoció la importancia de incluir un reconocimiento expreso a los derechos humanos de los usuarios digitales, que también pueden verse vulnerados en el ciber espacio o mediante el uso de las nuevas tecnologías de la información y la comunicación.

Así mismo, la Comisión discutió que alcance debían tener sus disposiciones, considerando que el ciberespacio es un ámbito virtual creado por tecnologías digitales interconectadas. Este nuevo dominio ha trastocado los conceptos tradicionales de jurisdicción territorial.

La utilización de redes y sistemas de información se está generalizando de manera acelerada. La digitalización y conectividad se están convirtiendo en elementos esenciales de un número cada vez mayor de productos y servicios. La Unión Europea señala que, con la llegada de la *internet de las cosas*, se espera que durante la próxima década se utilicen un número extremadamente alto de dispositivos digitales conectados. Mientras aumenta el número de dispositivos conectados a internet, la seguridad y la resiliencia no se tienen en cuenta de la misma manera, lo que provoca insuficiencias en la ciberseguridad.[18]

Por esta razón, junto al tradicional ámbito territorial nacional o de los lugares sometidos a su jurisdicción se consideró incluir: *o cuyos efectos se produzcan en el Ecuador.* Así, se reconoce la posibilidad de que la ley se aplique a las acciones que produzcan amenazas, riesgos o incidentes en redes, sistemas, infraestructuras o servicios ya sea que se encuentren operando en el país o desde el extranjero, cuando tengan efectos en el Ecuador o en los lugares sometidos a su jurisdicción.

5.6.2. Institucionalidad para la seguridad digital

La ley establece el Sistema Nacional de Seguridad Digital, el cual está integrado por:

1.- Instituciones públicas

2. Estrategias, normativas, planes, programas, políticas y servicios del sector público en todos los niveles del gobierno.

3.- personas naturales, jurídicas, privadas o comunitarias

[18] ANEXO 9: REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación punto (2). Disponible en: Disponible en: Reglamento (UE) 2019/ del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 (Reglamento sobre la Ciberseguridad) (europa.eu)

Cuando en sus actividades definan, coordinen, integren, ejecuten, supervisen, evalúen, controlen o sancionen el cumplimiento de la política de seguridad digital.

Este marco institucional tiene por fin promover la seguridad digital mediante la prevención, gestión e investigación de las amenazas, riesgos y delitos de naturaleza digital que afecten a la seguridad integral del Estado y al ejercicio de los derechos y libertades de sus ciudadanos en el ciberespacio, los sistemas informáticos y la red.

El Sistema Nacional de Seguridad Digital está integrado por 26 instituciones, las que a su vez se organizan en 4 subsistemas:

- Ciberseguridad ciudadana
- Ciberdefensa
- Ciberinteligencia
- Ciberdiplomacia

Uno de los aspectos más debatidos en este punto fue la rectoría del sistema, pues varias entidades responsables de los subsistemas tenían la predisposición de asumir esa facultad. Considerando que la lógica del sistema impide que una entidad sea al mismo tiempo responsable de un subsistema y cabeza del todo el sistema, se optó por conferir la rectoría al ministerio rector de las telecomunicaciones y de la sociedad de la información.

En efecto, el MINTEL ha desempeñado un rol protagónico en el desarrollo de la Estrategia Nacional de Seguridad Digital y otros instrumentos de política pública. Por tal motivo, se considera pertinente que sea la entidad que viene desarrollando las capacidades para ejercer el rol de ente rector, la que asuma esa alta responsabilidad.

A fin de facilitar la coordinación intersectorial, se crea un Comité Nacional de Seguridad Digital el cual es el encargado de la coordinación, transversalización, evaluación de la política pública integral de seguridad digital y la implementación de la estrategia nacional, la política pública y los planes nacionales para la reducción, respuesta y recuperación ante las amenazas, riesgos, incidentes, ataques o crisis que se puedan dar en el ciberespacio.

Este Comité está conformado por 11 entidades que se reúnen al menos una vez cada trimestre, cuenta con un secretario y tiene la posibilidad de activarse en caso de crisis y crear subcomités sectoriales o mesas técnicas de trabajo.

5.6.3. Gestión de Riegos e Incidentes Digitales

La digitalización de procesos analógicos e incluso de objetos tradicionalmente físicos, sumado a la conectividad acelerada y la penetración del internet trae consigo el aumento de riesgos en materia de ciberseguridad, ante la vulnerabilidad de la sociedad por su dependencia tecnológica.

La Unión Europea reconoce que reducir la dependencia de productos y servicios de ciberseguridad de fuera de la Unión y reforzar las cadenas de suministro al interior de sus estamos miembros es

un planteamiento estratégico que contribuye al desarrollo del sector de la ciberseguridad, en particular con las pymes, empresas emergentes, universidades y organismos de investigación.[19]

En este sentido, la gestión de incidentes constituye una actividad fundamental para la seguridad digital, y está organizada en 3 procesos principales:

1. Identificación y comprensión de vulnerabilidades, amenazas y riesgos
2. Respuesta a incidentes digitales
3. Recuperación ante incidentes

Es importante comprender que la gestión de riesgos e incidentes en el ciberespacio es responsabilidad de cada entidad regulada en la ley, por lo que deberán planificar e implementar procesos y acciones para identificar, analizar, evaluar y catalogar sus activos de información, incluyendo sus vulnerabilidades, amenazas y riesgos.

La respuesta a las vulnerabilidades, amenazas y riesgos que se presentan en el ciberespacio incluye la identificación, detección, análisis, evaluación, notificación, investigación o denuncia del incidente, así como la contención y neutralización ante ataques o vulneraciones de seguridad. De esta manera, la preparación para la respuesta involucra la alerta en los sistemas de seguridad, la evaluación del impacto del incidente y la determinación de probabilidades de ocurrencia de nuevos incidentes.

Finalmente, la recuperación de incidentes hace referencia, también, a la restauración de los activos de información al estado previo al incidente, la recuperación de sus estructuras y funciones básicas, así como el desarrollo o fortalecimiento de capacidades para su funcionamiento.

5.6.4. Instrumentos y herramientas para la seguridad digital

A nivel interno, la administración estatal se ha transformado en uno de los principales objetivos de los ataques digitales, por lo que constituye una inquietud de los integrantes de la Comisión el otorgar las herramientas necesarias al Estado para prevenir, mitigar, responder y recuperarse de los incidentes digitales.

La Unión Europa señala que los ciberataques van en aumento y que una sociedad más conectada es más vulnerable a amenazas en el ámbito digital; no obstante, mientras los ataques son transfronterizos, las competencias de las autoridades de ciberseguridad y policiales, así como las respuestas políticas a las mismas, se dan a nivel nacional. Por ello, resulta fundamental que los responsables políticos, la industria y los usuarios lleven a cabo una evaluación periódica del estado de la ciberseguridad y la resiliencia, basada en datos fiables y una previsión sistemática de los avances, retos y amenazas futuras. [20]

En consecuencia, el proyecto de ley abarca una serie de instrumentos que pueden ser agrupados, sin que ello implique una jerarquía, de la siguiente manera:

[19] Ibidem, punto (4)
[20] Ibidem, punto (5)

A nivel de política pública, el Plan Nacional y los Planes sectoriales de reducción, respuesta y recuperación ante riesgos, amenazas e incidentes digitales, la Estrategia Nacional de Seguridad Digital y las regulaciones y normas técnicas y protocolos de compartimentación de la información expedidas por las entidades correspondientes.

A nivel de herramientas operativas, las acreditaciones, la red de puntos de contacto, las certificaciones de buenas prácticas y el banco de incidentes.

A nivel de cultura de ciberseguridad, las plataformas de información y capacitación en seguridad digital y los ejercicios de ciberseguridad.

Finalmente, se deja abierta la posibilidad de que existan otros instrumentos creados por el ente rector del Sistema Nacional de Seguridad Digital.

5.6.5. Otros aspectos debatidos en el proyecto

Otros aspectos que fueron objeto de discusiones relevantes al interior de la Comisión, son los relativos a los mecanismos para acceder a la verdad de los hechos que, como fue señalado, constituye un eje transversal de todo el proyecto.

Para ello, en primer lugar, se ha reconocido el derecho a acceder a la verdad de los hechos en contextos digitales, pues la profusión de noticias falsas, la falta de respuestas finales respecto del cometimiento de ciberdelitos y la falta de identificación de sus posibles autores han generado la necesidad de establecer un nuevo paradigma en el manejo de la información, la trazabilidad de los sistemas, las huellas digitales que dejamos en el ciber espacio y hasta nuestra identidad virtual.

A fin de que este eje transversal no quede únicamente a nivel discursivo, se han sugerido una serie de buenas prácticas para promover el acceso a la verdad de los hechos, entre las que constan:

- La adopción de estándares técnicos, nacionales o internacionales, con énfasis en gobierno digital;
- La cultura de riesgo y resiliencia;
- La digitalización de procesos;
- La digitalización del 100% de los archivos institucionales;
- Los sistemas de identificación y seguimiento virtual de solicitudes y trámites ciudadanos;
- El acceso en línea directo a información de ejecución presupuestaria institucional cuatrimestral o balances financieros anuales;
- Los mecanismos de participación y decisión para el cumplimiento de presupuestos participativos;
- El espacio virtual de denuncias de actos de corrupción; y,
- Los mecanismos interactivos virtuales de formación que fomenten la cultura, historia y otros que determine el ente rector del Sistema Nacional de Seguridad Digital que permitan promover el acceso a la verdad de los hechos.

En el capítulo VI relativo a los instrumentos y mecanismos para el acceso a la verdad de los hechos, se ha incluido una Sección Tercera relativa al Financiamiento del Sistema Nacional de Seguridad Digital que incluye un "Fondo para la Seguridad Digital, Seguridad Sistémica y Acceso a la Verdad de los Hechos".

Sin perjuicio de las objeciones de constitucionalidad que puedan surgir respecto de la creación de gasto presupuestario a través de un proyecto de ley que no es iniciativa del Ejecutivo, la Comisión llama la atención respecto que la propia Constitución establece en su artículo 298 que:

*Se establecen preasignaciones presupuestarias destinadas a los gobiernos autónomos descentralizados, al sector salud, al sector educación, a la educación superior; y a la investigación, ciencia, **tecnología** e innovación en los términos previstos en la ley. Las transferencias correspondientes a preasignaciones serán predecibles y automáticas. Se prohíbe crear otras preasignaciones presupuestarias.*

Por lo cual, la Comisión ha resuelto establecer que las asignaciones que tenga el Sistema Nacional de Seguridad Digital, su funcionamiento, las políticas públicas de ciberseguridad, seguridad sistémica y acceso a la verdad de los hechos, así como la aplicación de los instrumentos del Sistema se financiarán mediante el Fondo para la Ciberseguridad, respecto del cual se espera conocer los criterios de los legisladores en el Pleno, a fin de determinar el correcto camino para dar aplicación a la disposición constitucional citada.

6. CONCLUSIONES DEL INFORME

El Proyecto de Ley Orgánica de Seguridad Digital cumple con las disposiciones constitucionales y legales que habilitan su presentación ante el Pleno de la Asamblea Nacional como un proyecto de ley independiente e integral.

7. RECOMENDACIONES DEL INFORME

Sobre la base del análisis y conclusiones que anteceden, la Comisión recomienda:

1. Aprobar el presente informe y continuar el tratamiento del Proyecto de Ley Orgánica de Seguridad Digital, como una ley autónoma no integrada al Código Orgánico de Seguridad del Estado.

2. Remitir a la presidencia de la Asamblea Nacional el presente informe a fin de que sea distribuido a las y los asambleístas y continúe el respectivo trámite parlamentario como proyecto de ley independiente.

8. RESOLUCIÓN Y DETALLE DE LA VOTACIÓN DEL INFORME

La Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral RESUELVE:

1. Aprobar el Informe para Primer Debate de la Ley Orgánica de Seguridad Digital con las conclusiones y recomendaciones expuestas.

2. Disponer al señor secretario de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral remita el presente informe con sus anexos al señor Presidente de la Asamblea Nacional, para su difusión al Pleno de la Asamblea Nacional.

Voluntad que se expresa en la siguiente votación:

Tabla 6: Detalle de la votación del informe

N°	ASAMBLEÍSTA	A FAVOR	EN CONTRA	BLANCO	ABSTENCIÓN
1	Simón Remache	✓			
2	Rodrigo Fajardo	✓			
3	Stalin Bayas	✓			
4	Xavier Jurado				
5	Patricia Núñez	✓			
6	Jorge Pinto	✓			
7	José Luis Vallejo	✓			
8	Geraldine Weber	✓			
9	Ramiro Narváez	✓			
Total		8			

9. ASAMBLEÍSTA PONENTE

El Asambleísta ponente será el Presidente de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, Asambleísta Ramiro Narváez Garzón.

10. NOMBRE Y FIRMA DE LAS Y LOS ASAMBLEÍSTAS QUE SUSCRIBEN EL INFORME

N°	ASAMBLEÍSTA	FIRMA
1	Simón Bolívar Remache	

2	Rodrigo Fajardo	Firmado electrónicamente por: RODRIGO OLMEDO FAJARDO CAMPOVERDE
3	Stalin Bayas	Firmado electrónicamente por: STALIN EFRAIN BAYAS TINE
4	Xavier Jurado	
5	Patricia Núñez	SILVIA PATRICIA NUNEZ RAMOS Firmado digitalmente por SILVIA PATRICIA NUNEZ RAMOS Fecha: 2023.03.23 14:58:30 -05'00'
6	Jorge Pinto	Firmado electrónicamente por: JORGE WASHINGTON PINTO DAVILA
7	José Luis Vallejo	Firmado electrónicamente por: JOSE LUIS VALLEJO AYALA
8	Geraldine Weber	Firmado electrónicamente por: GERALDINE WEBER MORENO

9	Ramiro Narváez	Firmado electrónicamente por: RAMIRO VLADIMIR NARVAEZ GARZON

11. PROYECTO DE LEY APROBADO PARA PRIMER DEBATE

PROYECTO DE LEY ORGÁNICA DE SEGURIDAD DIGITAL

EXPOSICIÓN DE MOTIVOS

En la actualidad, el uso de las tecnologías digitales ha revolucionado la forma en que nos comunicamos, trabajamos, aprendemos y nos entretenemos. Sin embargo, esta revolución tecnológica también ha llevado consigo nuevos riesgos y amenazas para la seguridad digital de las personas, empresas e instituciones.

En la era digital, la seguridad en línea es una necesidad cada vez más importante. A medida que más personas utilizan la tecnología y las empresas dependen cada vez más de ella, se hace evidente la necesidad de establecer leyes y regulaciones para proteger a los usuarios y empresas de los riesgos asociados con la seguridad digital.

De esta manera, es posible afirmar que los procesos de evolución o involución tecnológica a lo largo de la historia han generado importantes modificaciones en las estructuras sociales a tal punto de reinventar en algunos casos los *habitus* de producción y reproducción de la vida. La era de la conectividad en la que nos encontramos y cuyo antecedente exponencial se ubica en la última década del siglo pasado, viene vertiginosamente permeando todos los espacios de las relaciones sociales. En algunos casos aquel fenómeno ha permitido superar las limitaciones del tiempo-espacio, pero a la vez ha generado fisuras que ponen en riesgo o relativizan la protección de algunos derechos fundamentales.

Además, existen otras amenazas digitales, como el ciberacoso, el robo de identidad, el phishing, el malware y el ransomware. Estas amenazas pueden afectar a cualquier persona que utilice un dispositivo conectado a Internet, lo que incluye a grupos de atención prioritaria como niños, jóvenes y adultos mayores.

Además, la pandemia de COVID-19 ha llevado a un aumento significativo en el uso de la tecnología para el trabajo remoto y la educación a distancia. Este cambio ha creado nuevos riesgos de seguridad, como el aumento de los ataques de phishing y la exposición de información confidencial

a través de plataformas en línea. Por lo tanto, es crucial que los gobiernos adopte medidas concretas para abordar estos desafíos y garantizar que los ciudadanos puedan utilizar la tecnología de manera segura.

En la región países como Colombia, Brasil, Chile, Argentina, Perú han desarrollado normas, estrategias, ratificación de instrumentos internacionales como el Convenio de Budapest, políticas nacionales de ciberseguridad, ciberdefensa, ciberinteligencia, con el objetivo fundamental de garantizar la seguridad del ciberespacio como parte de la seguridad nacional, con cooperación internacional.

A nivel institucional, en Ecuador se ha conformado el Comité Nacional de Ciberseguridad; y, a nivel de política pública se ha expedido la Política y la Estrategia Nacional de Ciberseguridad. Sin duda y a pesar de estos avances, el estado de maduración de nuestro país en ciberseguridad demanda aún esfuerzos importantes.

A la necesidad de política pública, se suma la importancia de una adecuada regulación ante la creciente dependencia que tenemos de los sistemas informáticos, los cuales contienen una gran cantidad de información valiosa y confidencial. Por ejemplo, las empresas manejan datos personales de sus clientes, como nombres, direcciones y números de identificación, que pueden ser utilizados con fines malintencionados si caen en manos equivocadas. Asimismo, las instituciones gubernamentales y los hospitales manejan información sensible, como datos médicos y financieros, que también deben ser protegidos.

En relación al índice de ciberseguridad del año 2020 de la Unión Internacional de Telecomunicaciones, el Ecuador se ubica en el puesto 19 de la región detrás de Surinam, Guayana y Venezuela, mientras que a nivel mundial se ubica en la posición 119 de 182 países evaluados[21] aquel índice evalúa las medidas de legales, técnicas, organizacionales, de capacitación y cooperación respecto a la ciberseguridad, en las referidas variables Ecuador obtiene cero puntos en relación a las medidas organizacionales y cooperativas, seguido de un puntaje bajo en relación a la capacitación.[22]

El Reporte de Ciberseguridad 2020 establece que Ecuador tiene un 57% de penetración de internet, estableciendo una escala de indicadores del 1 al 5, se evidencia que: el desarrollo de la Estrategia de Nacional de Seguridad Cibernética desde el 2016 alcanza una puntuación de 2, se ha logrado identificar un 60% incidentes pero el modo de respuesta apenas alcanza 2 puntos de la escala. La protección de la infraestructura crítica (IC) fluctúa entre el 1 y 2 punto, el manejo de las crisis se ubica en 1 punto.[23] En un ejercicio de abstracción, considerando los 53 indicadores analizados en el Reporte de Ciberseguridad 2020, el Ecuador alcanza una puntuación de 1,77 sobre 5, es decir alcanza 94 puntos de una nota máxima de 265 puntos.[24]

[21] «Global Cybersecurity Index 2020», s. f., 172
[22] «Global Cybersecurity Index 2020», 61
[23] Observatorio de Ciberseguridad, OEA - BID, «Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe», 2020, 94.
[24] Observatorio de Ciberseguridad, OEA - BID, 94-95.

En Ecuador, el 17 de septiembre de 2019 se registró una falla informática que exponía los datos de alrededor de 17 millones de ciudadanos,[25] aquel hecho motivó la Ley de Datos Personales, sin embargo, esos esfuerzos legislativos deben ser complementados. En el marco de la pandemia se registró un aumento de ciberataques; y, en el año 2021 ha reflejado que Ecuador es el país de Latinoamérica con mayor aumento de ciberataques registrando un 75% en comparación a mediciones anteriores.[26]

En el Ecuador, la necesidad de una ley para la seguridad digital es evidente. Según el informe de amenazas cibernéticas de Kaspersky Security Network, se registraron más de 8,7 millones de ataques cibernéticos en Ecuador solo en el año 2020. Además, según la Encuesta Nacional de Victimización y Percepción de Seguridad Ciudadana, el 60% de los ecuatorianos reportó haber sido víctima de algún tipo de delito cibernético en los últimos doce meses; y, el 70% de las empresas ecuatorianas han sufrido algún tipo de ciberataque en los últimos dos años, lo que pone en evidencia la importancia de contar con medidas efectivas para proteger a las empresas y sus clientes.

A pesar de estos datos alarmantes, Ecuador aún no cuenta con una ley integral de seguridad digital. El país cuenta con algunas leyes y regulaciones relacionadas con la seguridad digital, como la Ley Orgánica de Telecomunicaciones, la Ley de Comercio Electrónico o la Ley Orgánica de Protección de Datos Personales. A estas leyes se suman las recientes reformas al Código Orgánico Integral Penal. Sin embargo, estas leyes no son suficientes para abordar los desafíos de la seguridad digital en la actualidad.

La falta de regulaciones específicas en este campo en Ecuador ha dejado a muchas personas y organizaciones vulnerables a los ataques cibernéticos como los recientes a la Corporación Nacional de Telecomunicaciones, Agencia Nacional de Tránsito o instituciones del sistema financiero.

En esta línea, la Comisión de Seguridad Integral de la Asamblea Nacional ha priorizado varias iniciativas orientadas a fortalecer la legislación para la seguridad digital. En este marco, la Comisión aprobó una Resolución que exhorta al Gobierno ecuatoriano a realizar todos los esfuerzos para la adhesión al Convenio de Budapest y sus protocolos.

La Comisión, también, tramitó el Proyecto de Ley Orgánica Reformatoria a Varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral, en la que reformó el Código Integral Penal e incorporó disposiciones para la búsqueda, preservación y tratamiento de la evidencia digital, así como normas para fortalecer la cooperación internacional, la investigación penal en el ciber espacio, el marco de actuación del agente encubierto informático, entre otras.

Así mismo, la Comisión elaboró reformas a la Ley de Telecomunicaciones para establecer la responsabilidad de los proveedores de servicios en la preservación del contenido digital.

[25] «Falla informática en Ecuador: los datos de casi toda la población quedaron expuestos», France 24, 17 de septiembre de 2019, https://www.france24.com/es/20190917-ecuador-datos-expuestos-informacion-filtracion
[26] Valentín Díaz, «Ecuador es el país de Latinoamérica con mayor aumento en ciberataques», El Comercio, 31 de agosto de 2021, https://www.elcomercio.com/actualidad/seguridad/ecuador-latinoamerica-aumento-ciberataques-kaspersky.html

El Ecuador está obligado a armonizar normas comunes con la región, definiendo procedimientos, mecanismos de cooperación y acciones conjuntas en función de garantizar la ciberseguridad, ciberdefensa, ciberinteligencia.

Es necesario que nuestro país cuente con subsistemas, mecanismos, estrategias de detección, prevención y reacción de los incidentes en el sistema digital, articulando a las instituciones de seguridad, defensa, inteligencia, para poder manejar las diferentes crisis de ciberseguridad, ciberdefensa y ciberinteligencia de manera ágil, oportuna, efectiva, eficiente y coordinada, con la finalidad de proteger las infraestructuras tecnológicas, infraestructuras críticas y servicios esenciales del Estado y de sus ciudadanos, y así también prevenir el cometimiento de ilícitos ante amenazas, riesgos y ataques en el ciberespacio.

Es indispensable, en consecuencia, que nuestro país resguarde la seguridad ciudadana, la soberanía del Estado, en el ciberespacio y se pueda prevenir, investigar, mitigar, actuar efectivamente ante el cometimiento, riesgo, ataque de delitos cibernéticos. Sin dejar a un lado el factor que actualmente muchos delitos se articulan, planean y ejecutan con y desde sistemas operativos, y dispositivos tecnológicos.

El Proyecto de Ley inscrito en el deber constitucional del Estado de garantizar el derecho a una cultura de paz, la seguridad integral y a vivir en una sociedad democrática y libre de corrupción,[27] desarrolla el eje 3 "Seguridad Integral" del Plan Nacional de Desarrollo vigente, específicamente en los objetivos 9 y 10 orientados a garantizar la seguridad ciudadana, orden público y gestión de riegos;[28] y, garantizar la soberanía nacional, integridad territorial y seguridad del Estado.[29]

El presente proyecto de Ley aborda una serie de temas importantes para enfrentar las amenazas digitales y la creación de un marco regulatorio claro para la seguridad digital en el Ecuador.

La Ley establece los principios que regulan la temática de seguridad digital, así como cuenta con un glosario de definiciones y actividades protegidas que incluye, entre otros: infraestructura crítica, estratégica y servicios esenciales; los sistemas de información de alto impacto; soberanía y defensa en el ciberespacio; derechos digitales frente al ciberdelito; diplomacia en el ciberespacio; y, cultura de seguridad digital.

Así mismo, la Ley determina nueve enfoques que debe tener la seguridad digital: planificación estratégica, integral, sistémico, multisectorial, multidimensional, de desarrollo sostenible, de derechos digitales, de resiliencia, de gobernanza y de confianza digital.

De otra parte, la Ley desarrolla la gestión de riesgos e incidentes digitales, a fin de garantizar la identificación y comprensión de vulnerabilidades, amenazas y riesgos, respuesta y recuperación ante incidentes digitales.

---

[27] Asamblea Nacional Constituyente, «Constitución de la República del Ecuador» (2008), Art. 3 numeral 8.
[28] Presidencia de la República del Ecuador, «Plan Nacional de Desarrollo 2021-2025 "Plan de Creación de Oportunidades"» (2021), 76.
[29] Presidencia de la República del Ecuador, 79.

Esta ley establece y regula el Sistema Nacional de Seguridad Digital y sus subsistemas de: ciberdefensa, ciberseguridad ciudadana, ciberinteligencia; y, ciberdiplomacia.

Crea así mismo, el Comité Nacional de Seguridad Digital como instancia de coordinación interinstitucional; y, el Centro de Respuesta a Incidentes de Seguridad Digital como entidad centralizada para la gestión de incidentes y, establece las atribuciones de todas las entidades del Sistema.

Norma los mecanismos y herramientas institucionales para promover la seguridad digital del Estado, la confianza digital, la cultura de seguridad en el ciberespacio y la protección de derechos humanos. Así mismo, la ley establece los instrumentos del sistema nacional de seguridad digital y mecanismos para el acceso a la verdad de los hechos.

Al respecto en la era de la hiperconectividad, el hiper-registro y las infodemias,[30] es un reto civilizatorio recuperar la *verdad de los hechos* como un mecanismo que permita superar la profundización de sociedades esquizofrénicas, es decir, la ciberseguridad, la seguridad sistémica; y, la verdad de los hechos, debe orientarse a combatir *la pos verdad* y debe permitir que las decisiones colectivas puedan ser tomadas de manera informada en tutela de los derechos fundamentales.

Por último, la Ley busca promover la educación y una cultura en seguridad digital, tanto para los ciudadanos como para las empresas e instituciones.

Es importante resaltar que el presente Proyecto de Ley, no incrementa el presupuesto económico del Estado, no crea institucionalidad, ni imposibilita el cumplimiento de las funciones de los organismos del Estados, otorga seguridad jurídica para poder actuar bajo amenazas, ataques en la red, en respeto de los principios y garantías constitucionales.

[30] Pandemia de información (intoxicación de información).

EL PLENO DE LA ASAMBLEA NACIONAL DE LA REPÚBLICA DEL ECUADOR

CONSIDERANDO

Que el artículo 1 de la Constitución de la República del Ecuador establece que "El Ecuador es un Estado constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico. Se organiza en forma de república y se gobierna de manera descentralizada";

Que la Constitución de la República del Ecuador, en su artículo 3 relativo a los deberes primordiales del Estado, entre otros, determina los deberes de "1. Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales (…)"; 8. Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción";

Que el artículo 6 de la Norma Suprema establece que "Todas las ecuatorianas y los ecuatorianos son ciudadanos y gozarán de los derechos establecidos en la Constitución";

Que el artículo 16 del Texto Supremo señala que "Todas las personas, en forma individual o colectiva, tienen derecho a: (…) 2. El acceso universal a las tecnología de información y comunicación".

Que el artículo 84 de la Constitución de la República establece que la "Asamblea Nacional y todo órgano con potestad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano o de las comunidades, pueblos y nacionalidades. En ningún caso, la reforma de la Constitución, las leyes, otras normas jurídicas ni los actos del poder público atentarán contra los derechos que reconoce la Constitución";

Que el número 6 del artículo 120 de la Constitución de la República del Ecuador establece como atribución y deber de la Asamblea Nacional, expedir, codificar, reformar y derogar las leyes, e interpretarlas con carácter generalmente obligatorio;

Que el artículo 132 de la Norma Suprema, establece a Asamblea Nacional aprobará como leyes las normas generales de interés común (…) Se requerirá de ley en los siguientes casos: "1. Regular el ejercicio de los derechos y garantías constitucionales";

Que el artículo 133, de la Norma constitucional, establece que serán leyes orgánicas: "2. Las que regulen el ejercicio de los derechos y garantías constitucionales";

Que el artículo 226 de la Constitución de la República del Ecuador establece: "Las entidades del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que

actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la Ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución";

Que el artículo 227 de la Constitución de la República del Ecuador dispone que la administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación;

Que de conformidad con el artículo 277 de la Constitución de la República, para la consecución del buen vivir, es deber del Estado promover e impulsar la ciencia, la tecnología, las artes, los saberes ancestrales y en general las actividades de la iniciativa creativa comunitaria, asociativa, cooperativa y privada.;

Que el artículo 298 del texto constitucional señala que: "Se establecen preasignaciones presupuestarias destinadas a los gobiernos autónomos descentralizados, al sector salud, al sector educación, a la educación superior; y a la investigación, ciencia, **tecnología** e innovación en los términos previstos en la ley. Las transferencias correspondientes a preasignaciones serán predecibles y automáticas. Se prohíbe crear otras preasignaciones presupuestarias".

Que el artículo 385 de la Carta Suprema establece que El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad: 1. Generar, adaptar y difundir conocimientos científicos y tecnológicos. 2. Recuperar, fortalecer y potenciar los saberes ancestrales. 3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir".

Que el artículo 424 de la Constitución de la República, establece que "La Constitución es la norma suprema y prevalece sobre cualquier otra del ordenamiento jurídico. Las normas y los actos del poder público deberán mantener conformidad con las disposiciones constitucionales; en caso contrario carecerán de eficacia jurídica (…)"

Que la Ley Orgánica de Telecomunicaciones establece en su artículo 15 que: "Son deberes de los prestadores de servicios de telecomunicaciones, con independencia del título habilitante del cual se derive tal carácter, los siguientes: 1. Garantizar el acceso igualitario y no discriminatorio a cualquier persona que requiera sus servicios.2. Prestar el servicio de forma obligatoria, general, uniforme, eficiente, continua, regular, accesible y responsable, cumpliendo las regulaciones que dicte la Agencia de Regulación y Control de las Telecomunicaciones y lo establecido en los títulos habilitantes. (…) 4. Respetar los derechos de los usuarios establecidos en esta Ley y en el ordenamiento jurídico vigente. (…) 9. Cumplir con las obligaciones de acceso universal y servicio universal determinados en los correspondientes títulos habilitantes. (…) 12. Cumplir con las obligaciones de interconexión, acceso y ocupación de conformidad con esta Ley, su Reglamento General y las normas técnicas y disposiciones

respectivas. 13. Garantizar el secreto e inviolabilidad de las comunicaciones cursadas a través de las redes y servicios de telecomunicaciones, sin perjuicio de las excepciones establecidas en las leyes.14. Adoptar las medidas necesarias para la protección de los datos personales de sus usuarios y abonados, de conformidad con esta Ley, su Reglamento General y las normas técnicas y regulaciones respectivas. 15. Adoptar las medidas para garantizar la seguridad de las redes. (…) 25. Conservar la información relacionada con la prestación de servicios de telecomunicaciones, en las condiciones y por el tiempo que se disponga en las regulaciones respectivas. (…)".

Que la Ley Orgánica de Telecomunicaciones establece en su artículo 66 que: "La interconexión y el acceso deberán realizarse de conformidad con principios de igualdad, no-discriminación, neutralidad, buena fe, transparencia, publicidad y sobre la base de costos".

Que la Ley Orgánica de Telecomunicaciones establece en su artículo 79 que: "En caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de telecomunicaciones, el prestador de servicios de telecomunicaciones informará a sus abonados, clientes y usuarios sobre dicho riesgo y sobre las medidas a adoptar".

Que la Ley Orgánica de Protección de Datos Personales señala que en su artículo 1 señala que: "El objeto y finalidad de la presente Ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela".

En ejercicio de las atribuciones establecidas en el artículo 120 numeral 6 de la Constitución de la República, Art. 54 y conexos, relacionados con el procedimiento legislativo prescritos en la Ley Orgánica de la Función Legislativa, expide la siguiente:

Título

PRELIMINAR

Capítulo I

OBJETO, ÁMBITO Y FINALIDADES

Artículo 1. Objeto.- La presente Ley tiene por objeto establecer los procesos para la prevención, identificación, mitigación, respuesta y resiliencia frente a las amenazas, riesgos e incidentes en el ciberespacio u otros entornos digitales; establece y regula el Sistema Nacional de Seguridad Digital y sus subsistemas de ciberseguridad, ciberdefensa, ciberinteligencia y ciberdiplomacia; y, norma los mecanismos y herramientas institucionales para promover la seguridad del Estado, la confianza digital, la cultura de seguridad en el ciberespacio y la protección de derechos humanos.

Artículo 2. Ámbito.- Las disposiciones de esta Ley son de orden público y de obligatorio cumplimiento a nivel nacional para todos los organismos y dependencias de las funciones del Estado; las entidades que integran el régimen autónomo descentralizado y las personas jurídicas creadas por ellos; los organismos creados por la Constitución y la Ley para el ejercicio de la potestad estatal,

la prestación de servicios públicos o el desarrollo de actividades económicas; las personas naturales y jurídicas públicas y privadas que realizan actividades en el ciberespacio u otros entornos digitales.

La presente ley se aplicará frente a las amenazas, riesgos o incidentes en redes, sistemas, infraestructuras o servicios que se encuentren operando o prestándose dentro del territorio nacional o cuyos efectos se produzcan en el Ecuador o en los lugares sometidos a su jurisdicción.

Las disposiciones de la presente ley son aplicables sin perjuicio del cumplimiento de las disposiciones de la Ley Orgánica de Protección de Datos Personales.

Artículo 3. Finalidades de la Ley.- Son finalidades de esta ley:

1. Fortalecer y proteger la soberanía, seguridad integral, infraestructuras críticas y servicios esenciales públicos y privados y fomentar la resiliencia de los sistemas de información en el entorno digital.

2. Promover la seguridad digital de las personas naturales y jurídicas públicas y privadas en el ciberespacio u otros entornos digitales mediante la gestión integral de riesgos y amenazas.

3. Regular el Sistema Nacional de Seguridad Digital y los subsistemas de ciberseguridad, ciberdefensa, ciberinteligencia y ciberdiplomacia y la participación del sector público y privado.

4. Establecer procedimientos para identificar, determinar las características y gestionar los incidentes a nivel nacional de manera sistémica.

5. Proveer al Estado la capacidad para prevenir, organizar, coordinar y hacer operativa la respuesta y resiliencia ante riesgos, amenazas o incidentes en el ciberespacio.

6. Desarrollar los lineamientos para la elaboración, aprobación y evaluación de la estrategia y de la política nacional de seguridad digital y promover su cumplimiento.

7. Promover la asistencia, colaboración y cooperación nacional e internacional para alcanzar la seguridad sistémica en el ciberespacio.

8. Garantizar el acceso a la verdad de los hechos y fomentar una cultura de la ciberseguridad responsable en la ciudadanía, mediante el desarrollo de capacidades en ciberseguridad.

9. Promover la confianza para el intercambio de información y la gestión de conocimiento en seguridad en el ciberespacio.

10. Establecer los requisitos normativos específicos de ciberseguridad y la obligación de implementación de buenas prácticas de los actores sujetos a esta Ley.

Capítulo II

PRINCIPIOS Y DEFINICIONES

Artículo 4. Principios.- La aplicación de la presente ley se rige por los principios previstos en la Constitución de la República, los instrumentos internacionales vigente en Ecuador y los siguientes principios específicos:

Autenticidad.- En todo momento se garantizará que las y los emisores de datos relativos al tráfico puedan ser identificables. En la seguridad de un ordenador, la autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador.

Cooperación.- Las entidades, personas naturales y jurídicas públicas y privadas dentro del ciberespacio cooperarán para generar mejores condiciones de seguridad digital, seguridad sistémica y acceso a la verdad de los hechos. En el marco del respecto a la soberanía nacional, la cooperación también será interinstitucional e internacional en los términos establecidos en la presente Ley y en los instrumentos internacionales vigentes en el Ecuador.

Disponibilidad.- Con fines de seguridad digital, seguridad sistémica y acceso a la verdad de los hechos, se garantizará la búsqueda, el acceso, la preservación y la utilización del contenido digital. Es deber de todas y todos los obligados garantizar la disponibilidad de la información con las reservas y condiciones que la Ley establezca.

Las autoridades del Estado, de conformidad con la ley y los instrumentos internacionales aplicables, pondrán solicitar y poner a disposición de las autoridades de otro Estado u organismos internacionales, la información necesaria para prevenir las amenazas y ataques.

Integridad.- Es la precisión, consistencia y confiabilidad de los datos o contenido digital durante su ciclo de vida, por lo cual no deben ser modificados, manipulados, dañados, deteriorados, alterados, suprimidos o borrados durante la transferencia o almacenamiento por entidades no autorizadas.

Oportunidad.- Las acciones de prevención, contención y las medidas de no repetición deberán ejecutarse con urgencia, necesidad, proporcionalidad y responderán a la gravedad de los amenazas, riesgos o incidentes.

Reserva de la Información.- Se deberá mantener la compartimentación de las operaciones en los ámbitos de seguridad y defensa, de los activos de información digital, así como la reserva en las estrategias y acciones desarrolladas y se respetará el carácter confidencial de la información clasificada, sin embargo, no podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas.

La información de cualquier índole, como estudios, antecedentes, datos, documentos e informes que obtengan, elaboren, recopilen o intercambien los órganos que conforman el Sistema Nacional de Seguridad Digital serán empleados para el cumplimiento de los objetivos institucionales.

Artículo 5. Definiciones.- En la aplicación de la presente Ley se observarán las siguientes definiciones:

Auditoría de ciberseguridad.- Es el estudio periódico de cumplimiento para determinar la garantía de ciberseguridad al que se someterán las y los sujetos, redes, infraestructuras y sistemas que determine la presente Ley.

Catálogo Nacional de Infraestructuras Estratégicas y Críticas.- Es la información completa, actualizada, contrastada e informáticamente sistematizada, relativa a las características específicas de cada una de las infraestructuras críticas existentes en el territorio nacional.

Amenaza.- Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste mediante la cual se pretende vulnerar una red, sistema o infraestructura con finalidades contrarias a la Ley.

Ataque.- Conjunto de actividades no autorizadas y maliciosas producidas en el ciberespacio que comprometen la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan, ejecutadas mediante el uso de las tecnologías de la información y comunicación, que vulneren los activos de información y que afecten la seguridad integral del Estado o vulneren una red, sistema o infraestructura privada para atacar a los sistemas y servicios presentes en el mismo o alcanzables a través suyo.

Ciberdefensa.- Capacidad militar, intelectual y tecnológica que poseen las Fuerzas Armadas para ejecutar operaciones en y a través del ciberespacio, que permitan explorar, proteger y defender de ciberataques a la infraestructura crítica e información estratégica del Estado, así como apoyar el cumplimiento de operaciones para la defensa de la soberanía y la integridad territorial.

Ciberdelincuencia.- Es la actividad delictiva de alcance nacional o transnacional, en la que se utiliza tecnologías de la información y comunicación como objeto o medio para perpetuar un delito.

Ciberdelito.- Conducta típica, antijuridica y culposa mediante la utilización de cualquier medio tecnológico, dispositivo informático o electrónico que ponga en peligro la seguridad de los activos de los sistemas de información o comunicación o cualquier otro bien jurídico protegido.

Ciberdiplomacia.- Son las acciones realizadas por el ente rector del relaciones exteriores y movilidad humana a fin de contribuir la seguridad digital, a la lucha contra el ciberdelito internacional en aplicación de derecho internacional, promoviendo las medidas de fomento de la confianza, representando la posición nacional ante organizaciones y foros internacionales y regionales y promoviendo las relaciones multilaterales y bilaterales en los campos de la seguridad digital y supervisar la cooperación para el desarrollo en el ámbito digital.

Ciberespacio.- Dominio global y dinámico compuesto por infraestructuras de tecnología de la información incluyendo internet, redes de telecomunicaciones y sistemas de información.

Ciberespionaje.- Conjunto de actividades originadas o patrocinadas por Estados, organizaciones, grupos, empresas o individuos conocidos o desconocidos, con la intención de apropiarse de

información sensible o valiosa que afecte la seguridad integral del estado por el cual un usuario accede a contenido para el cual no se encuentra autorizado dentro del ciberespacio o actos maliciosos que buscan causar daño accediendo a un sistema informático desde y en el ciberespacio.

Ciberinteligencia.- Actividades del Sistema Nacional de Inteligencia que utilizan todas las fuentes de inteligencia en apoyo de la seguridad digital para caracterizar su amenaza en general, recopilar las intenciones y posibilidades de los adversarios potenciales, analizar, identificar, localizar, determinar y comunicar la fuente de las vulnerabilidades, amenazas, incidentes y ataques.

Ciberseguridad.- Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan.

Vulnerabilidad.- Constituye la omisión o anomia de una red, infraestructura o sistema que significan un riesgo de ciberseguridad en el ciberespacio o la debilidad en los procedimientos de seguridad de un sistema de información. Esta debilidad podría explotarse accidental o intencionadamente para violar los controles o la política de seguridad de dicho sistema.

Crisis.- Una crisis en el ciberespacio es el resultado de un incidente o una cadena de incidentes que provocan la interrupción de una operación crítica o de infraestructura crítica, estratégica o servicio esencial que, a su vez, pone en riesgo la vida o la salud de muchas personas, provoca daños patrimoniales y ambientales importantes o interferencias severas y extensas en la continuidad de los servicios u operaciones vitales, y cuya resolución requiere la pronta actuación coordinada.

Datos relativos al tráfico.- Son todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Datos informáticos.- Es toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programadas diseñados para que un sistema informático ejecute una función.

Entorno digital.- Término que se refiere e incluye a usuarios, redes, dispositivos, software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a redes de comunicaciones o sistemas de información electrónicos.

Infraestructura digital.- Abarca a los sistemas de hardware, software, instalaciones y componentes de servicio que respaldan la entrega de servicios, tales como data centers y redes de comunicaciones, así como los componentes necesarios para operar y administrar los entornos públicos o privados.

Infraestructura crítica.- Es la infraestructura física o digital, elemento, sistema o parte de este situado en el Estado o donde el Estado ejerce soberanía que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad integral, y el bienestar social y

económico de la población, cuya perturbación o destrucción afectaría gravemente al Estado al no poder mantener esas funciones.

Infraestructura estratégica.- Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

Servicio esencial-. Es el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas que dependa para su provisión de redes y sistemas de información.

Sistema informático.- Es todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Proveedor de servicios.- Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, redes, infraestructura y servicios de telecomunicaciones que prestan el servicio de acceso a internet y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de este.

Tecnologías de la información y la comunicación (TIC's).- Son aquellos recursos y herramientas que se utilizan para el proceso, administración y distribución de la información a través de elementos tecnológicos.

Trazabilidad.- Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Capítulo III

Actividades protegidas

Artículo 6. **Actividades protegidas.-** La presente ley protege:

a. La infraestructura crítica, estratégica y servicios esenciales;
b. Los sistemas de información de alto impacto;
c. Soberanía y defensa en el ciberespacio;
d. Derechos digitales frente al ciberdelito;
e. Diplomacia en el ciberespacio; y,
f. Cultura de seguridad digital.

Artículo 7. ***Infraestructura crítica, estratégica y servicios esenciales.-*** Se protege las infraestructuras críticas y estratégicas del sector público o privado, consideradas como vitales para el desarrollo del país y que puedan ser vulneradas en el ciberespacio; además, protege los servicios esenciales establecidos en Ecuador cuando su residencia o domicilio se encuentre en territorio

ecuatoriano y cuya afectación, denegación, interrupción o destrucción pueden tener consecuencias negativas para la participación en democracia, gobernabilidad, el régimen de desarrollo o las relaciones internacionales, impactando en el bienestar de la ciudadanía en general.

Artículo 8. **Activos de información de alto impacto.-** Se protege los activos de información que son fundamentales para las actividades de entidades públicas y privadas y los activos de información de los proveedores de servicios digitales que tengan su residencia o domicilio en el territorio ecuatoriano, frente a las amenazas que afecten a estos activos impactando la confidencialidad, integridad y disponibilidad de los datos y la entrega y calidad de los servicios no esenciales.

Artículo 9. Soberanía y defensa en el ciberespacio.- Se protege y defiende los activos de información, infraestructura, servicios y actividades cuya afectación puede atentar contra la soberanía del Estado, frente a las amenazas y riesgos provenientes del ciberespacio u otros entornos.

Artículo 10. Derechos frente al ciberdelito.- Se protege los derechos en general y en particular los derechos digitales de las personas ante los riesgos y amenazas que conlleven al cometimiento de ciberdelitos y delitos cometidos por medio de las tecnologías de la información y comunicación.

Artículo 11. Diplomacia en el ciberespacio.- Se protege y fomenta los procesos y seguridad de la información de los órganos del servicio exterior, agregadurías, procesos electorales, oficinas comerciales y, en general, servicios prestados por el Estado ecuatoriano fuera del país; frente a las amenazas y riesgos del ciberespacio que son transnacionales y requieren ser abordados a través de la cooperación internacional, el fortalecimiento de la confianza y la seguridad internacionales.

Artículo 12. Cultura de ciberseguridad.- Se protege y fomenta las actividades de difusión, capacitación y formación cuyo objetivo sea la construcción de una cultura de ciberseguridad en el país que permitan generar una conciencia compartida de identificación de riesgos y amenazas en el ciberespacio, toma de medidas preventivas y de respuesta; resiliencia digital y la toma de decisiones estratégicas con base en la recolección, procesamiento y análisis de la información para la prospección y anticipación a las amenazas, riesgos e incidentes informáticos.

Capítulo IV

ENFOQUES DE LA SEGURIDAD DIGITAL

Artículo 13. Enfoque de planificación estratégica.- La seguridad digital se orientará por el Plan Nacional de Seguridad Integral y la Estrategia Nacional de Seguridad Digital que reflejará la visión del Estado y de la sociedad ecuatoriana respecto de los objetivos en materia de seguridad de la información en el ciberespacio, los resultados esperados y el alcance de las actividades a implementar.

Artículo 14. Enfoque integral.- La seguridad digital se preservará desde un enfoque integral que se base en el entendimiento y análisis global del entorno digital, adaptado a las circunstancias del país y considerando todas las dimensiones de la seguridad integral.

Artículo 15. Enfoque sistémico.- La seguridad digital se asegurará considerando un contexto sistémico, interdependiente, conexo y polivalente, que permita comprender la interrelación de todos sus aspectos. Los sujetos obligados por la presente Ley adoptarán medidas para garantizar el cumplimiento material de la misma mediante sistemas integrados u otras acciones con la debida diligencia.

Artículo 16. Enfoque multisectorial y multidimensional.- Dado el carácter transversal de la seguridad digital, las políticas públicas, planes, proyectos y acciones incluirá a los distintos actores del sistema, tanto del sector público como privado o comunitario, conforme al modelo de gobernanza participativa que será inclusivo, transparente y que permitirá afrontar la responsabilidad de la gestión los riesgos digitales de manera compartida.

Artículo 17. Enfoque de desarrollo sostenible.- La seguridad digital contribuirá al crecimiento económico, desarrollo económico y el desarrollo sostenible, a través de la facilitación, entre otros, de los servicios públicos, el comercio internacional y el progreso tecnológico, en articulación con los objetivos de desarrollo acordados por la comunidad internacional y Plan Nacional de Desarrollo.

Artículo 18. Enfoque de derechos digitales.- En la aplicación de la ley y el desarrollo de las políticas públicas se garantizará el ejercicio de los derechos digitales y demás derechos reconocidos en la Constitución de la República y los instrumentos internacionales de derechos humanos suscritos por el Ecuador.

Cuando la seguridad digital implique la eventual vigilancia, interceptación de las comunicaciones, tratamiento o recopilación de datos, estas actividades se efectuarán exclusivamente en el contexto de una investigación, causa judicial o previa autorización de autoridad competente.

Artículo 19. Enfoque de resiliencia.- Las políticas, planes, programas, proyectos y acciones para la seguridad digital fomentarán la generación de capacidades para que las entidades públicas y privadas que conforman el Sistema Nacional de Seguridad Digital respondan y se recuperen, de manera oportuna y eficiente, de un incidente o ataque informático y tomen las medidas de reparación, en particular mediante la preservación y la restauración de sus estructuras y funciones básicas.

Artículo 20. Enfoque de gobernanza.- Para promover la seguridad digital todos los actores del sistema incluyendo a la sociedad civil, las empresas privadas y las personas naturales nacionales o extranjeras y todas las funciones públicas y los diferentes niveles de gobierno del régimen seccional descentralizado, articularan, colaborarán y ejecutarán acciones para la reducción, respuesta y recuperación ante las amenazas, riesgos, incidentes y ataques provenientes del ciberespacio.

Artículo 21. Enfoque de confianza digital.- La seguridad digital buscará promover la confianza en el entorno digital mediante la garantía de la seguridad de la información de los activos de información aprovechando las oportunidades que ofrecen las tecnologías de la información y comunicación, tecnologías de operación y tecnologías emergentes para el desarrollo del entorno digital.

Capítulo V

GESTIÓN DE RIESGOS E INCIDENTES DIGITALES

Artículo 22. **Gestión de riesgos e incidentes en el ámbito digital.-** La gestión de riesgos e incidentes en el ámbito digital, se realizará de manera integral y sistémica, considerando los siguientes procesos principales:

1. Identificación y comprensión de vulnerabilidades, amenazas y riesgos
2. Respuesta a incidentes digitales
3. Recuperación ante incidentes

Las entidades sujetas a esta ley implementarán los procesos de gestión de riesgos e incidentes para prevenir y reducir los niveles de riesgo y vulnerabilidad.

Artículo 23. **Identificación y comprensión de vulnerabilidades, amenazas y riesgos.-** Las entidades reguladas en esta ley, en el marco de sus respectivas competencias y responsabilidades planificarán e implementarán procesos y acciones para identificar, analizar, evaluar y catalogar los activos de información, sus vulnerabilidades, amenazas y riesgos.

Artículo 24. **Respuesta a incidentes digitales .-** La respuesta ante incidentes en el ciberespacio u otros entornos digitales integra, entre otros, los subprocesos de preparación para la respuesta; identificación, detección, análisis, evaluación, notificación, investigación o denuncia del incidente; así como la contención y neutralización ante ataques o vulneraciones de seguridad.

La preparación para la respuesta permite gestionar las vulnerabilidades asegurando los activos de información, la gestión de la comunicación, la identificación de elementos de seguridad, la evaluación de capacidades de detección de amenazas y la determinación de recursos para la mitigación.

La identificación, detección, análisis, evaluación, notificación, investigación o denuncia de incidentes permite la identificación de alertas en los sistemas de seguridad, la evaluación del impacto del incidente, el conocimiento, determinación de probabilidad de ocurrencia de nuevos incidentes, así como la declaración, notificación, investigación o denuncia de los incidentes.

Las contención y neutralización incorpora acciones para evitar la propagación del incidente, el incremento de su impacto y la disminución de los daños.

Artículo 25. **Recuperación ante incidentes digitales.-** El proceso de recuperación integra los subprocesos y componentes que permiten la restauración de los activos de información al estado previo al incidente; la recuperación de sus estructuras y funciones básicas o el desarrollo y fortalecimiento de capacidades para su funcionamiento.

Este proceso permite el diseño de estrategias, políticas, planes, programas, proyectos para el aumento de la resiliencia, la prevención y la reducción de nuevos riesgos.

TITULO II

SISTEMA NACIONAL DE SEGURIDAD DIGITAL

Capítulo I

SISTEMA NACIONAL DE SEGURIDAD DIGITAL

Artículo 26. Sistema Nacional de Seguridad Digital.- El Sistema Nacional de Seguridad Digital es el conjunto articulado y coordinado de subsistemas, instituciones, estrategias, normativas, planes, programas, políticas y servicios del sector público en todos los niveles del gobierno, personas naturales, jurídicas, privadas o comunitarias que definen, coordinan, integran, ejecutan, supervisan, evalúan, controlan o sancionan el cumplimiento de la política de seguridad digital.

El Sistema Nacional de Seguridad Digital tiene por fin de promover la seguridad digital mediante la prevención, gestión e investigación de las amenazas, riesgos y delitos de naturaleza digital que afecten a la seguridad integral del Estado y al ejercicio de los derechos y libertades de sus ciudadanos en el ciberespacio, los sistemas informáticos y la red.

Artículo 27. Integración del Sistema Nacional de Seguridad Digital.- El Sistema Nacional de Seguridad Digital estará integrado por las siguientes instituciones y organismos:

1. El ministerio rector de las telecomunicaciones y de la sociedad de la información;
2. El ente responsable de la coordinación de la seguridad pública y del Estado;
3. El ministerio rector de la política pública de defensa nacional;
4. El Comando Conjunto de Fuerzas Armadas;
5. El ministerio rector de seguridad ciudadana, protección interna y orden pública;
6. Policía Nacional;
7. El ente rector del Sistema Nacional de Inteligencia;
8. El ente rector de la política exterior y movilidad humana;
9. El ente rector del Sistema Nacional de Rehabilitación Social;
10. El ente rector en materia de gestión de riesgos;
11. La Agencia de Regulación y Control de las Telecomunicaciones;
12. El Sistema Integrado de Seguridad ECU 911 o quien haga sus veces;
13. El Consejo de la Judicatura;
14. La Fiscalía General del Estado;
15. La Autoridad de Protección de Datos Personales;
16. Las superintendencias del país;
17. El Instituto Ecuatoriano de Normalización o el que haga sus veces;
18. Las entidades públicas o privadas que administren, operen o proveen infraestructura crítica, estratégica o servicios esenciales;
19. Los gobiernos autónomos descentralizados en todos sus niveles;
20. La Unidad de Análisis Financiero y Económico o quien haga sus veces;
21. El Servicio de Rentas Internas o quien haga sus veces;
22. El Servicio Nacional de Aduana del Ecuador o quien haga sus veces;
23. La Agencia Nacional de Tránsito;
24. Las y los responsables de seguridad digital de las entidades públicas y privadas con presencia en el ciberespacio;
25. Las y los responsables de seguridad digital de las entidades con infraestructura crítica; y,
26. Las demás entidades y actores definidas por el Comité Nacional de Seguridad Digital.

De manera eventual, podrá formar parte cualquier otro organismo o institución involucrado que se requiera para los fines de ciberseguridad, ciberdefensa, ciberinteligencia y ciberdiplomacia.

Artículo 28. Organización del Sistema Nacional de Seguridad Digital.- El Sistema Nacional de Seguridad Digital estará organizado en subsistemas que se encargarán, de acuerdo con el ámbito de sus competencias, de precautelar y garantizar la ciberseguridad, ciberdefensa, ciberinteligencia y ciberdiplomacia.

Artículo 29. Funciones generales de las instituciones del Sistema.- A las entidades y actores del Sistema Nacional de Seguridad Digital, en el marco de sus atribuciones, competencias y responsabilidades les corresponde:

1. Identificar y evaluar las vulnerabilidades y los escenarios de riesgos que puedan afectar la seguridad digital con la finalidad de reducir, prevenir, detectar, mitigar, gestionar, responder, contener y recuperarse de las amenazas, riesgos, incidentes, ataques o crisis que se puedan dar en el ciberespacio;
2. Definir e implementar medidas de preparación, planificación y coordinación con otras entidades públicas y privadas involucradas para cumplir las finalidades del sistema;
3. Brindar asesoría en materia de seguridad digital a la Función Ejecutiva, al Consejo de Seguridad Pública y del Estado y a las otras funciones del Estado, cuando así le sea requerido;
4. Proveer insumos para la formulación de la política pública de seguridad digital y contribuir en la implementación de la estrategia nacional y la política pública de seguridad digital;
5. Articular y coordinar acciones con todas las entidades del Sistema Nacional de Seguridad digital para prevenir, reducir, responder, y promover la recuperación resiliente ante amenazas, riesgos, incidentes, ataques o crisis digitales;
6. Promover la confianza en el entorno digital, la cultura de seguridad digital en el país; y, el acceso a la verdad de los hechos;
7. Establecer mecanismos y estrategias de financiamiento para las acciones de prevención, respuesta y recuperación ante amenazas, riesgos, incidentes, ataques o crisis digitales;
8. Elaborar y presentar informes en materia de seguridad digital, ante las entidades de rectoría y coordinación del Sistema Nacional de Seguridad Digital;
9. Cumplir las disposiciones, directrices, normas técnicas, lineamientos expedidos por las entidades de rectoría, gestión y coordinación;
10. Nombrar al responsable de seguridad digital de la entidad y crear las unidades de seguridad digital, de conformidad con las directrices expedidas por el ente rector del sistema;
11. Entregar la información requerida por las entidades de rectoría y regulación, necesaria para garantizar la seguridad digital;
12. Notificar a las entidades correspondientes los incidentes o ataques;
13. Establecer e implementar medidas para la prevención, respuesta, recuperación o combate ante la ciberdelincuencia;
14. Participar en los ejercicios de seguridad digital, definidos por la entidad rectora del Sistema o las entidades responsables de los subsistemas;

15. Alertar y denunciar a las autoridades competentes por los incidentes y delitos que se cometan en el ciberespacio y que afecten la soberanía y la seguridad ciudadana;
16. Colaborar con las entidades competentes en los procesos de investigación de ciberdelitos; y,
17. Cumplir con las demás funciones, atribuciones y responsabilidades establecidas en la presente ley, su reglamento general de aplicación y la normativa que se expida dentro del Sistema.

Estas funciones serán adicionales a las que les otorga las leyes, reglamentos y normativa interna de acuerdo con el ámbito de sus competencias.

Capítulo II

ENTIDADES DE RECTORÍA, COORDINACIÓN Y GESTIÓN INCIDENTES DIGITALES

Sesión Primera

RECTORÍA

Artículo 30. Rectoría del Sistema Nacional de Seguridad Digital.- La rectoría del sistema la tendrá el ministerio rector de las telecomunicaciones y de la sociedad de la información.

Artículo 31. Atribuciones del ente rector del Sistema Nacional de Seguridad Digital.- El ministerio rector de las telecomunicaciones y la sociedad de la información, en el ámbito de la seguridad digital, tendrá las siguientes funciones y atribuciones :

1. Elaborar, en coordinación con los demás actores del sistema, la estrategia nacional, la política pública y los planes de acción para reducción, respuesta y recuperación ante amenazas, riesgos, incidentes, ataques o crisis que se puedan dar en el ciberespacio;
2. Cumplir con las resoluciones del Comité Nacional de Seguridad Digital;
3. Elaborar para aprobación del Comité Nacional de Seguridad Digital, el Plan Nacional de Seguridad Digital el que será de carácter bianual y estará alineado al Plan Nacional de Desarrollo y al Plan Nacional de Seguridad Integral y supervisar su cumplimiento;
4. Expedir normativa y directrices para la supervisión y control en el ámbito de la seguridad digital;
5. Promover la observancia y cumplimiento de todas las obligaciones internacionales en materia de seguridad digital;
6. Diseñar y proponer para aprobación del Comité Nacional de Seguridad Digital, los procedimientos para identificar los activos de información críticos y que permitan la provisión de servicios esenciales;
7. Asegurar la actuación coordinada de los subsistemas para prevenir, gestionar y eliminar cualquier acto que atente contra la ciberseguridad, ciberdefensa, ciberinteligencia y ciberdiplomacia;
8. Reglamentar la realización de auditorías para la seguridad de la información en el ámbito público y privado;
9. Identificar y regular a los operadores de servicios de telecomunicaciones para reducción de amenaza y riesgos en el ciberespacio, la respuesta ante incidentes y ataques digitales y la comunicación de emergencia;

10. Presentar las estrategias preventivas y de respuesta al Presidente de la República y al Consejo de Seguridad Publica y del Estado en materia de seguridad digital.
11. Crear, fortalecer y evaluar al Centro Nacional de Respuesta a Incidentes Informáticos, ciberataques y crisis digitales;
12. Crear e institucionalizar el observatorio del ciberespacio para recopilar, analizar y clasificar la información sobre amenazas e incidentes;
13. Diseñar y ejecutar programas nacionales de sensibilización y cultura en materia de seguridad digital;
14. Promover o coordinar procesos de formación en seguridad digital, seguridad sistémica y acceso a la verdad de los hechos en el marco de sus atribuciones;
15. Fomentar la creación de programas de apoyo para la prevención y combate del ciberdelito y del ciberterrorismo;
16. Promover el mejoramiento de las capacidades de los subsistemas;
17. Proponer al Comité Nacional de Seguridad Digital, acciones, políticas, requerimientos estratégicos, equipamiento o medidas en el marco de sus atribuciones para garantizar la seguridad digital y fortalecer la seguridad de la infraestructura crítica;
18. Monitorear y reportar el estado de los medios y herramientas informáticas y de tecnologías de la información y comunicación en los organismos del sector público;
19. Establecer, por interés público, regulaciones para el registro de dispositivos electrónicos en el ámbito público y privado a fin de contribuir al combate a la ciberdelincuencia y el ciberterrorismo;
20. Establecer un sistema estadístico permanente de registro, seguimiento y monitoreo de los incidentes y ataques a las entidades a su cargo y reportar al Comité Nacional de Seguridad Digital;
21. Emitir boletines y alertas de seguridad digital, seguridad sistémica y acceso a la verdad de los hechos;
22. Elaborar estrategias y protocolos para garantizar seguridad digital, seguridad sistémica y acceso a la verdad de los hechos que serán puestos en consideración del Comité Nacional de Seguridad Digital;
23. Compilar, actualizar y elaborar anualmente el banco de alertas que será puesto a consideración del Comité Nacional de Seguridad Digital para su aprobación;
24. Supervisar el cumplimiento de las normativas de seguridad digital, seguridad sistémica y acceso a la verdad de los hechos de todas las entidades obligadas en el Sistema Nacional de Seguridad Digital;
25. Recomendar la suscripción de acuerdos y convenios internacionales interinstitucionales en materia de ciberseguridad, ciberdefensa, ciberinteligencia y ciberdiplomacia;
26. Las demás establecidas en la Ley, el reglamento general de aplicación y por el Comité Nacional de Seguridad Digital.

Estas funciones serán adicionales a las otorgadas en leyes, reglamentos y normativa interna de acuerdo con el ámbito de sus competencias.

Sección Segunda

COORDINACIÓN INTERSECTORIAL

Artículo 32. Comité Nacional de Seguridad Digital.- El Comité Nacional Seguridad Digital es el organismo estratégico, colegiado, de coordinación, transversalización, evaluación política pública integral de seguridad digital y toma de decisiones, responsable de la implementación de la estrategia nacional, la política pública y los planes nacionales para la reducción, respuesta y recuperación ante las amenazas, riesgos, incidentes, ataques o crisis que se puedan dar en el ciberespacio.

Artículo 33. Conformación del Comité Nacional de Seguridad Digital.- El Comité Nacional de Seguridad Digital estará conformado por:

1. La máxima autoridad del ente rector del sistema de seguridad digital quien gozará de voto dirimente;
2. El ente responsable de la coordinación de la política pública de seguridad integral o su delegado permanente;
3. La máxima autoridad la Secretaría General de la Administración Pública o su delegado permanente;
4. La máxima autoridad del ente rector de la defensa nacional o su delegado permanente;
5. La máxima autoridad del ente rector de seguridad ciudadana, protección interna y orden público o su delegado permanente;
6. La máxima autoridad del ente rector del Sistema Nacional de Inteligencia o su delegado permanente;
7. La máxima autoridad del ente rector de las relaciones exteriores y movilidad humana o su delegado permanente;
8. La máxima autoridad de la Secretaría General de la Administración Pública y Gabinete de la Presidencia de la República o su delegado permanente;
9. La máxima autoridad de la Agencia de Regulación y Control de las Telecomunicaciones o su delegado permanente;
10. La máxima autoridad del Consejo de la Judicatura o su delegado permanente; y,
11. La máxima autoridad de la Fiscalía General del Estado o su delegado permanente.

Las y los integrantes del Comité Nacional de Seguridad Cibernética tendrán voz y voto en todas las decisiones del organismo. En cualquier momento a solicitud de un integrante del Comité o, de oficio, quien preside el órgano colegiado requerirá y autorizará la participación de expertas o expertos quienes ejercerán derecho a voz sin voto en las sesiones del Comité.

La secretaria o el secretario del Comité Nacional de Seguridad Digital se elegirá entre las máximas autoridades o sus delegados permanentes.

El reglamento a la presente ley establecerá la organización y funcionamiento del Comité.

Artículo 34. Atribuciones del Comité Nacional de Seguridad Digital.- El Comité Nacional de Seguridad Digital tendrán las siguientes atribuciones:

1. Aprobar, transversalizar, coordinar e implementar la Plan Nacional de Seguridad Digital, Estrategia Nacional, el Plan de Implementación de la Estrategia Nacional, y demás instrumentos de política pública para la reducción, respuesta y recuperación ante amenazas, riesgos, incidentes, ataques o crisis en el ciberespacio;

2. Supervisar y coordinar el cumplimiento de las funciones por parte de los organismos miembros del Sistema Nacional de Seguridad Digital;
3. Conocer y resolver respecto de los informes de cumplimiento del Plan Nacional de Seguridad Digital y Plan de Implementación de la Estrategia Nacional y desarrollar herramientas de seguimiento y evaluación;
4. Participar en el proceso de formulación, implementación y evaluación de las políticas públicas, planes, programas y proyectos para la reducción, respuesta y recuperación ante amenazas, riesgos, incidentes, ataques o crisis en el ciberespacio;
5. Asesorar y orientar a los máximos niveles gubernamentales en la gestión integral de la seguridad digital;
6. Establecer normas nacionales y estándares para los operadores de infraestructuras críticas digitales en el sector público y privado;
7. Aprobar y actualizar la metodología para la identificación y medidas de protección de las infraestructuras estratégica y críticas con enfoque intersectorial e inclusivo;
8. Aprobar anualmente el catálogo nacional de infraestructura crítica y estratégica y servicios esenciales que, excepcionalmente, en cualquier momento podrá actualizarse bajo solicitud motivada del Consejo de Seguridad Pública y del Estado o el que haga sus veces;
9. Solicitar la declaratoria de zona de seguridad a los lugares donde se encuentre la infraestructura estratégica o digital que provea servicios esenciales, acorde a lo determinado en la ley;
10. Definir mecanismos de cooperación y coordinación gubernamental, internacional y entre el sector público, privado, asociativo, cooperativo y la academia;
11. Aprobar el sistema de alerta temprana y el banco de incidentes para la detección y registro de amenazas y riesgos en el ciberespacio;
12. Aprobar los protocolos de respuesta y recuperación de acuerdo con el nivel y tipo de incidente, ataque o crisis en el ciber espacio;
13. Establecer mecanismos para la divulgación periódica de amenazas y el intercambio de información entre prestadores de servicios esenciales de infraestructura crítica y el gobierno nacional;
14. Conocer y aprobar el Informe Nacional Anual del Estado de la Seguridad Digital en el Ecuador que incluya las medidas de no repetición adoptadas;
15. Establecer las estrategias de financiamiento y recursos para garantizar la Seguridad Digital;
16. Proponer medidas y estrategias que en el ámbito de la seguridad digital permitan garantizar los derechos digitales y el acceso a la verdad de los hechos;
17. Aprobar la normativa correspondiente a las certificaciones de seguridad digital, que incluirá el diseño y actualización del esquema de certificación orientado a preservar la seguridad digital;
18. Proponer, cuando corresponda, análisis en materia de seguridad digital y acceso a la verdad de los hechos;
19. Calificar sus decisiones como información clasificada, conforme a los criterios y al procedimiento establecido en la ley de la materia;
20. Normar los criterios y especificidades técnicas para la realización de ejercicios prácticos de seguridad digital;
21. Desarrollar normas, estándares, incentivos de mercado, esquemas voluntarios de cumplimiento y otras iniciativas para aumentar la confianza digital;

22. Determinar los requerimientos estratégicos y los recursos necesarios para garantizar seguridad digital, seguridad sistémica y acceso a la verdad de los hechos;
23. Suscribir o sugerir a las instituciones la subscripción de acuerdos y convenios internacionales interinstitucionales en materia de seguridad digital, sin perjuicio de las atribuciones que tengan las entidades conforme a la normativa correspondiente;
24. Aprobar anualmente el informe de seguimiento sobre incidente, ataques y amenazas que incluirá el estado judicial procesal de conformidad con la reglamentación emitida para el efecto y que considerará los niveles de clasificación por razones de seguridad pública y del Estado;
25. Promover propuestas legislativas relacionadas con seguridad digital, seguridad sistémica y acceso a la verdad de los hechos;
26. Aprobar los criterios técnicos para la creación y funcionamiento del banco de alertas;
27. Aprobar las metodologías, procesos y controles a nivel nacional para garantizar la seguridad digital, mediante un mecanismo de evaluación de las medidas de seguridad; y,
28. Las demás establecidas en la Ley y su reglamento general de aplicación.

Artículo 35. Funcionamiento del Comité Nacional de Seguridad Digital.- El Comité Nacional de Seguridad Digital se reunirá de manera ordinaria al menos una vez cada trimestre por convocatoria de su presidente o por solicitud de la mitad más uno de las y los delegados que lo conforman.

El Comité Nacional de Seguridad Digital expedirá la normativa para su funcionamiento que deberá incluir, entre otros aspectos, la periodicidad de las reuniones y su activación en caso de crisis; convocatoria; designación de autoridades; mecanismos de toma de decisión; creación de subcomités sectoriales, mesas técnicas de trabajo; lugar de reuniones; mecanismos de acreditación de las y los delegados institucionales; régimen de ausencias y justificaciones; posibilidad de pedido de sustitución de la delegada o delegado; estrategias de articulación; difusión de la información; y, demás aspectos que faciliten su organización y funcionamiento.

Artículo 36. Secretaría del Comité Nacional de Seguridad .- El secretario del Comité Nacional de Seguridad Digital será nombrado de entre las o los servidores de la Entidad Rectora del Sistema Nacional de Seguridad Digital y durará en el cargo por un período de dos años, renovable por una sola vez.

Artículo 37. Funciones de la Secretaría del Comité Nacional de Seguridad Digital.- Además de las que establece la Ley deberá cumplir:

1. Convocar a las sesiones de Comité Nacional de Seguridad Digital por disposición de su presidenta o presidente;
2. Elaborar las actas de las sesiones y suscribirlas junto a la presidenta o presidente del Comité Nacional de Seguridad Digital;
3. Llevar el registro de actas y archivo físico o digital de la documentación del Comité Nacional de Seguridad Digital garantizando la memoria histórica de la Institución; incluyendo los convenios de cooperación nacionales e internacionales que estarán a disposición de las instituciones del sistema, conforme al reglamento a esta ley;

4. Servir de enlace entre las distintas entidades que conforman en Comité Nacional de Seguridad Digital,
5. Certificar las actuaciones y los documentos del Comité Nacional de Seguridad Digital;
6. Elaborar las respuestas a los pedidos de información de las resoluciones y actividades del Comité Nacional de Seguridad Digital;
7. Poner a disposición de la ciudadanía la información no clasificada del trabajo del Comité Nacional de Seguridad Digital, a través de los medios tecnológicos definidos para el efecto;
8. Dar seguimiento a los acuerdos y resoluciones del Comité Nacional de Seguridad Digital; y,
9. Las demás establecidas en el reglamento general de aplicación a esta ley y a la normativa para el funcionamiento del Comité Nacional de Seguridad Digital.

Artículo 38. Ente coordinador de las entidades del Sistema de Seguridad Pública y del Estado.- El ente coordinador de las entidades que integran el Sistema de Seguridad Pública y del Estado, facilitará la coordinación del Sistema de Seguridad Pública y del Estado o el que lo reemplace con el Sistema Nacional de Seguridad Digital

Sección Tercera

GESTIÓN DE INCIDENTES DIGITALES

Artículo 39. Centro de Respuesta a Incidentes de Seguridad Digital.- El Centro de Respuestas a Incidentes de Seguridad Digital es la entidad única y centralizada, con competencia para la gestión integral de incidentes digitales. Se creará de conformidad con la normativa que expida el ente rector del Sistema Nacional de Seguridad Digital.

En su funcionamiento, coordina y articula esfuerzos con entidades sectoriales, nacionales e internacionales para la vigilancia, prevención, respuesta y recuperación ante incidentes en el ciberespacio, proporcionando análisis periódicos de riesgos en ciberseguridad e incidentes y coordinando la respuesta a nivel nacional.

Artículo 40. Funciones del Centro Nacional de Respuesta a Incidentes de Seguridad Digital.- Son funciones del Centro Nacional de Respuesta a Incidentes de Seguridad Digital las siguientes:

1. Conformar equipos especiales y específicos de respuesta de acuerdo con el nivel y a la naturaleza de los incidentes en el ciberespacio;
2. Coordinar y articular acciones con los centros de respuesta a incidentes de las entidades públicas y privadas;
3. Definir protocolos y realizar entrenamientos y ejercicios prácticos conjuntos internacionales, nacionales y sectoriales de seguridad digital;
4. Realizar ejercicios que involucren escenarios de contingencia;
5. Implementar y operar el sistema de alerta temprana y el banco de incidentes para la detección y registro de vulnerabilidades, amenazas y riesgos;
6. Elaborar los informes periódicos de alertas, de cibervulnerabilidades, riesgos, amenazas e incidentes que le sean requeridos;

7. Proponer al Comité Nacional de Seguridad Digital e implementar los protocolos de respuesta y recuperación de acuerdo con el nivel y tipo de incidente;
8. Participar en foros e iniciativas regionales y multilaterales sobre normativa internacional, medidas de fomento de la confianza y creación de capacidades en materia de seguridad digital; y
9. Otras definidas por el ente rector del sistema o el Comité Nacional de Seguridad Digital.

Artículo 41. Gestión integral e intersectorial de respuesta a incidentes cibernéticos.- La respuesta a incidentes se gestionará de manera integral e intersectorial, a través de subsistemas que se encargarán, de acuerdo al ámbito de sus competencias, de la detección, análisis, evaluación y notificación de incidentes, así como la contención y neutralización, en los ámbitos de ciberdefensa, ciberseguridad, ciberinteligencia y ciberdiplomacia.

Capítulo III

Subsistemas del Sistema Nacional de Seguridad Digital

Sección Primera

SUBSISTEMA DE CIBERDEFENSA

Artículo 42. Subsistema de Ciberdefensa.- El Subsistema de Ciberdefensa estará conformado por el ministerio rector de la Defensa Nacional y la unidad respectiva del Comando Conjunto de las Fuerzas Armadas.

El Subsistema de Ciberdefensa tendrá coordinación y colaboración directa con los subsistemas de ciberdiplomacia, ciberseguridad y ciberinteligencia, que entregarán la información necesaria para el correcto cumplimiento de las funciones del subsistema de ciberdefensa, para la defensa, reducción, respuesta y recuperación frente a riesgos, amenazas, incidentes en el ciberespacio cuando tengan relación con la soberanía del Estado.

Artículo 43. Ente ejecutor de la política de ciberdefensa.- El Ministerio rector de la Defensa Nacional o quien haga sus veces, será responsable de la política pública en materia de ciberdefensa, para lo cual articulará sus actuaciones con el Comité Nacional de Seguridad Digital y las demás entidades y actores del Sistema Nacional de Seguridad Digital.

Artículo 44. Atribuciones del ente rector de la Defensa Nacional.- Además de las atribuciones propias de la cartera de Estado y las funciones generales de las instituciones del Sistema Nacional de Seguridad Digital, el ente rector de la Defensa Nacional tendrá las siguientes atribuciones en materia de ciberdefensa:

1. Gestionar y coordinar la ciberdefensa mediante acciones intergubernamentales e interinstitucionales;
2. Cumplir con las políticas públicas, estrategias, planes y acciones determinadas por el Comité Nacional Seguridad Digital y el ente rector del Sistema Nacional de Seguridad Digital;
3. Definir e implementar planes, programas y proyectos para el mejoramiento de las capacidades de ciberdefensa, de conformidad con los lineamientos y directrices del Comité y ente rector del Sistema Nacional de Seguridad Digital;

4. Elaborar el componente de ciberdefensa para su incorporación en el Plan Nacional y la Estrategia Nacional de Seguridad Digital;
5. Fortalecer la capacidad estratégica de ciberdefensa de Fuerzas Armadas;
6. Recopilar, procesar y analizar información con la finalidad proponer al Comité Nacional de Seguridad Digital, acciones, políticas o medidas en el marco de sus atribuciones para garantizar soberanía nacional, ciberdefensa, para la reducción, respuesta y recuperación ante amenazas, riesgos e incidentes;
7. Levantar el catálogo de servicios esenciales, infraestructura crítica nacional y áreas estratégicas;
8. Realizar la evaluación de las vulnerabilidades, en coordinación con los prestadores de servicios esenciales en infraestructuras críticas del Estado, en ciberdefensa de las instituciones del Estado, con la finalidad reportar al ente rector del Sistema y elaborar recomendaciones a los prestadores de servicios;
9. Analizar y determinar, con los niveles estratégicos de la defensa y demás entidades del Estado, los requerimientos relacionados con la ciberdefensa para presentar al Comité Nacional de Seguridad Digital;
10. Establecer un sistema institucional de registro, seguimiento y monitoreo de las vulnerabilidades, amenazas, riesgos e incidentes de las entidades a su cargo y reportar al Comité Nacional de Seguridad Digital;
11. Implementar un mecanismo de gestión y respuesta a incidentes que se articule al Centro Nacional de Respuesta a Incidentes de Seguridad Digital;
12. Responder ante las amenazas o ataques mediante acciones técnicas, oportunas y estratégicas, recopilar indicios; y, reportar los resultados al Comité Nacional de Seguridad Digital;
13. Identificar los componentes de infraestructura informática que poseen un alto riesgo en relación con la defensa nacional conforme a la normativa nacional correspondiente;
14. Coordinar con el Consejo de Seguridad Pública y del Estado o su equivalente para actualizar el catálogo de servicios esenciales, infraestructura crítica nacional y áreas estratégicas que, dependiendo de la clasificación respectiva, será puesta a consideración del Comité Nacional de Seguridad Digital;
15. Desarrollar proyectos de investigación y transferencia tecnológica con la finalidad de proteger y defender los servicios escenciales e infraestructura crítica del Estado;
16. Elaborar un registro evaluaciones y presentarlo anualmente al ente rector del Sistema Nacional de Seguridad Digital;
17. Desarrollar proyectos de investigación y transferencia tecnológica con la finalidad de prevenir incidentes, ataques a la soberanía del Estado en el ciberespacio;
18. Dirigir y supervisar, dentro de las entidades a su cargo, el desarrollo de las capacidades humanas y tecnológicas de ciberdefensa;
19. Planificar, realizar y participar en ejercicios para la ciberdefensa y la ciberseguridad, a nivel nacional e internacional;
20. Coordinar con entidades y organismos tanto públicos como privados e internacionales para el desarrollo de mecanismos de cooperación táctica y operativa para la protección y defensa de servicios esenciales e infraestructura crítica del Estado;
21. Garantizar la formación y capacitación de personal militar especializado para la defensa del Estado en y a través del ciberespacio;

22. Coordinar y apoyar la respuesta y recuperación ante delitos informáticos, ciberataques y otros incidentes cibernéticos que puedan afectar a las instituciones públicas y privadas, que pongan en riesgo la defensa, soberanía del Estado y las infraestructuras críticas;
23. Levantar escenarios prospectivos en base a las matrices de riesgo u otras metodologías para la identificación de amenazas en el ciberespacio y recomendar acciones estratégicas y operativas;
24. En coordinación con el Subsistema de Ciberinteligencia, definir las acciones y recursos, operativos y tácticos que permita contar con inteligencia estratégica para la ciberdefensa;
25. Preparar y ejecutar la planificación para la detección, prevención, contención y respuesta ante las nuevas amenazas digitales que traten de afectar las áreas críticas o estratégicas nacionales;
26. Promover procesos de formación en ciberdefensa, seguridad sistémica y acceso a la verdad de los hechos en el marco de sus atribuciones;
27. Gestionar y promover, en coordinación con el ente rector de las relaciones exteriores y movilidad humana, la cooperación internacional y nacional para fortalecer las capacidades estatales de reducción, respuesta y recuperación ante riesgos, amenazas, incidentes, ataques y crisis digitales que puedan poner en riesgo la soberanía, la integridad territorial, los recursos estratégicos del Estado y la seguridad del Estado y suscribir los acuerdos y convenios interinstitucionales en el ámbito de sus competencias;
28. Participar en foros e iniciativas regionales y multilaterales sobre normativa internacional, medidas de fomento de la confianza y creación de capacidades en materia de seguridad digital;
29. Remitir, anualmente, o cuando lo amerite, al responsable del subsistema de ciberdiplomacia, los requerimientos de cooperación internacional y,
30. Las demás establecidas en la Ley, el reglamento general de aplicación y las determinadas por el Comité Nacional de Seguridad Digital.

Estas atribuciones se ejecutarán de manera coordinada con el Comando Conjunto de las Fuerzas Armadas y serán adicionales a las que les otorga las leyes, reglamentos, normativa interna de acuerdo con el ámbito de sus competencias.

Sección Segunda

SUBSISTEMA DE CIBERSEGURIDAD CIUDADANA

Artículo 45. Subsistema de Ciberseguridad Ciudadana.- El Subsistema de Ciberseguridad Ciudana estará conformado por el ente rector de seguridad ciudadana, protección interna y orden público, la Policía Nacional del Ecuador, el ente rector del Sistema Nacional de Rehabilitación Social, la Fiscalía General del Estado y el Sistema Integrado de Seguridad Ecu 911 y otras entidades que se consideren necesarias para resguardar la seguridad ciudadana y protección interna en el ciberespacio.

El Subsistema de Ciberseguridad Ciudadana tendrá coordinación directa con los subsistemas de ciberdiplomacia, ciberdefensa y ciberinteligencia, que entregarán la información oportuna y

necesaria para el correcto cumplimiento de las funciones de este subsistema para la prevención, investigación y judicialización del ciberdelito y combate a la ciberdelincuencia.

El subsistema de Ciberseguridad Ciudadana articulará acciones y podrá solicitar información a todas las entidades del Sistema Nacional de Inteligencia de conformidad con la Ley.

El Subsistema establecerá mecanismos para la garantía del acceso a la verdad de los hechos, la no repetición y la no impunidad.

Artículo 46. Ente ejecutor de la política pública de ciberseguridad ciudadana.- El ente rector de seguridad ciudadana, orden público y protección interna o quien haga sus veces, será responsable de la política pública en materia de prevención, investigación y combate a la ciberdelincuencia, para lo cual articulará sus actuaciones con la entidad rectora del Sistema Nacional de Seguridad Digital, el Comité Nacional de Seguridad Digital y las demás entidades y actores del Sistema.

Artículo 47. Atribuciones del ente rector de *seguridad ciudadana, protección interna y orden público* ***en materia de ciberseguridad ciudadana.-*** Además de las atribuciones propias de la cartera de Estado y las funciones generales de las instituciones del Sistema Nacional de Seguridad Digital, el ente rector de seguridad ciudadana, protección interna y orden público tendrá las siguientes atribuciones y funciones:

1. Cumplir con las políticas públicas, estrategias, planes y acciones determinadas por el Comité Nacional Seguridad Digital y el ente rector del Sistema Nacional de Seguridad Digital;
2. Elaborar el componente de ciberseguridad ciudadana para la prevención, investigación y combate a la ciberdelincuencia para su incorporación en el Plan Nacional de Seguridad Digital y la Estrategia Nacional de Seguridad Digital;
3. Actuar como entidad responsable de la prevención, investigación y combate a la ciberdelincuencia;
4. Articular acciones con las demás entidades que conforman el Sistema Nacional de Seguridad Digital para la prevención, investigación y combate a la ciberdelincuencia;
5. Recopilar información de manera ágil y oportuna de las diferentes entidades públicas y privadas que se consideren necesarias para la prevención, investigación y combate a la ciberdelincuencia;
6. Definir e implementar planes, programas y proyectos para el mejoramiento de las capacidades de ciberseguridad para la prevención, investigación y combate a la ciberdelincuencia, de conformidad con los lineamientos y directrices del Comité y ente rector del Sistema Nacional de Seguridad Digital;
7. Recopilar, procesar y analizar información con la finalidad de proponer al Comité Nacional de Seguridad Digital, acciones, políticas o medidas en el marco de sus atribuciones para reducción, respuesta y recuperación frente a amenazas, riesgos, incidentes, prevención y combate a la ciberdelincuencia;
8. Realizar el análisis de vulnerabilidades en ciberseguridad, de las entidades del subsistema para resguardar la seguridad ciudadana en el ciberespacio, con la finalidad de presentar un informe de hallazgos y recomendaciones a ser implementadas;

9. Implementar un mecanismo de gestión y respuesta a los incidentes digitales, en el ámbito de sus competencias y que se articule al Centro Nacional de Respuesta a Incidentes de Seguridad Digital;
10. Establecer un sistema institucional de registro, seguimiento y monitoreo de las vulnerabilidades, amenazas, riesgos e incidentes de las entidades a su cargo y reportar al Comité Nacional de Seguridad Digital;
11. Responder a los ciberdelitos mediante acciones técnicas, oportunas y estratégicas, recopilar indicios o evidencias a través de la unidad pertinente de la Policía Nacional; y, reportar los resultados al Comité Nacional de Seguridad Digital, de acuerdo con la clasificación de la información;
12. Coordinar con entidades y organismos tanto públicos como privados e internacionales para que, de manera conjunta, se desarrollen mecanismos de cooperación táctica y operativa para la prevención, investigación y combate a la ciberdelincuencia;
13. Implementar un sistema integral con la Policía Nacional y otras entidades que se consideren necesarias para resguardar la seguridad ciudadana en el ciberespacio, a través del cual, se registren denuncias y las noticias del delito a escala nacional e internacional para determinar la influencia, tendencias, prácticas, modos de operación, perfiles criminales, alcance y caracterización, para la prevención, investigación y combate a la ciberdelincuencia;
14. Desarrollar proyectos de investigación y transferencia tecnológica con la finalidad de prevenir amenazas, riesgos, ataques, incidentes y ciberdelitos en el ciberespacio;
15. Promover procesos de formación para la ciudadanía con enfoque a la prevención del ciberdelito y acceso a la verdad de los hechos;
16. Apoyar la respuesta y recuperación ante ciberdelitos, ataques y otros incidentes digitales que puedan afectar a las instituciones públicas y privadas o los derechos de la ciudadanía;
17. Garantizar la formación y capacitación de los agentes encubiertos digitales;
18. Fortalecer las capacidades tecnológicas para la adquisición, materialización y preservación de la evidencia digital;
19. Realizar el registro, seguimiento y monitoreo de incidentes a las entidades a su cargo y reportar al Comité Nacional de Seguridad Digital;
20. Identificar en las entidades a su cargo los activos de información que posee un alto riesgo;
21. Desarrollar proyectos de investigación y transferencia tecnológica con la finalidad de prevenir amenazas, riesgos, ataques, incidentes y delitos informáticos en el ciberespacio;
22. Promover procesos de formación en ciberseguridad ciudadana y acceso a la verdad de los hechos en el marco de sus atribuciones;
23. En coordinación con el Subsistema de Ciberinteligencia, definir las acciones y recursos que permita contar con inteligencia estratégica para la ciberseguridad ciudadana;
24. Gestionar y promover, en coordinación con el ente rector de las relaciones exteriores y movilidad humana, la cooperación internacional y nacional para fortalecer las capacidades estatales de reducción, respuesta, recuperación ante riesgos, amenazas, incidentes y ciberdelitos que puedan poner en riesgo la seguridad ciudadana y el orden público; y suscribir los acuerdos y convenios interinstitucionales en el ámbito de sus competencias;
25. Participar en foros e iniciativas regionales y multilaterales sobre normativa internacional, medidas de fomento de la confianza y creación de capacidades en materia de seguridad digital;
26. Remitir, anualmente, o cuando lo amerite, al responsable del subsistema de ciberdiplomacia, los requerimientos de cooperación internacional; y

27. Las demás establecidas en la Ley, el reglamento general de aplicación y las determinadas por el Comité Nacional de Seguridad Digital.

Sección Tercera

SUBSISTEMA DE CIBERINTELIGENCIA

Artículo 48. Subsistema de Ciberinteligencia.- El Subsistema de Ciberinteligencia, apoyará al Sistema Nacional de Inteligencia y estará conformado por el ente rector en materia de inteligencia, la unidad de ciberdefensa del Comando Conjunto de las Fuerzas Armadas y las unidades o responsables de ciberinteligencia, de la Policía Nacional del Ecuador, del ente rector del Sistema Nacional de Rehabilitación Social, del Centro Nacional de Respuesta a Incidentes de Seguridad Digital, del Servicio de Rentas Internas, de la Unidad de Análisis Financiero y Económico, del Servicio Nacional de Aduana del Ecuador, del ente rector de telecomunicaciones y sociedad de la información y de la Casa Militar Presidencial o quien haga sus veces.

El Subsistema de Ciberinteligencia tendrá coordinación directa con el subsistema de ciberdefensa, el subsistema de ciberseguridad y subsistema de ciberdiplomacia y articulará acciones y requerirá la entrega obligatoria de información de las superintendencias, agencias de control, prestadores de servicios esenciales e infraestructura crítica, y del Centro Nacional de Respuesta a Incidentes de Seguridad Digital y otras entidades que deban entregar información en función de sus competencias, a fin de contar con información para identificación, alerta y respuesta ante amenazas que afecten la seguridad digital, seguridad ciudadana, contra la infraestructura estratégica, infraestructura crítica digital y los servicios esenciales.

Artículo 49. Ente ejecutor de la política pública de ciberinteligencia.- El ente rector en materia de inteligencia o quien haga sus veces, será responsable de la política pública en materia de ciberinteligencia, para lo cual articulará sus actuaciones con el Comité Nacional de Seguridad Digital y las demás entidades de este subsistema y actores del Sistema Nacional de Seguridad Digital.

Artículo 50. Atribuciones del ente rector del Sistema Nacional de Inteligencia. - Además de las atribuciones propias de la cartera de Estado y las funciones generales de las instituciones del Sistema Nacional de Seguridad Digital, el ente rector del Sistema Nacional de Inteligencia tendrá las siguientes funciones y atribuciones:

1. Proponer y cumplir con las políticas públicas, estrategias, planes y acciones determinadas por el Comité Nacional Seguridad Digital y el ente rector del Sistema Nacional de Seguridad Digital;
2. Establecer, en coordinación con el ente rector del Sistema Nacional de Seguridad Digital, las directrices para el manejo de información clasificada.
3. Establecer las directrices y acreditar los sistemas de información y comunicaciones para el manejo de información clasificada;
4. Asesorar a las máximas autoridades de las Funciones del Estado respecto de los planes, programas, proyectos, políticas públicas, acciones, estrategias, buenas prácticas u otros, para la protección de los intereses estratégicos del Estado y la sociedad en el ciberespacio;

5. Dar directrices y evaluar la implementación de planes, programas y proyectos para el mejoramiento de las capacidades de identificación de vulnerabilidades, amenazas y riesgos en seguridad digital de los integrantes del Subsistema;
6. Orientar y coordinar los requerimientos de búsqueda y obtención de información en fuentes abiertas y cerradas para la producción de ciberinteligencia estratégica;
7. Generar inteligencia estratégica del ciber espacio;
8. Intercambiar ciberinteligencia con servicios de inteligencia extranjeros, en el marco de la cooperación intergubernamental;
9. Recopilar, procesar y analizar información con la finalidad proponer al Comité Nacional de Seguridad Digital, recomendaciones de acciones, políticas o medidas en el marco de sus atribuciones para la repuesta y recuperación frente amenazas y riesgos en el ciberespacio, dependiendo de la clasificación de la información;
10. Coordinar y gestionar la realización de evaluaciones de vulnerabilidades, amenazas y riesgos en el nivel estratégico de las instituciones del Estado y en los miembros del subsistema de ciberinteligencia, con la finalidad de emitir, a cada uno, un informe clasificado que deberá contar con las acciones, medidas y recomendaciones a desarrollar para controlar posibles riesgos en el ciberespacio;
11. Apoyar en la respuesta a incidentes, mediante su análisis técnico, recopilación de indicios o evidencias y otras acciones que aporten a contener un incidente cuando sea requerido por instituciones públicas o privadas y, reportar los resultados al Comité Nacional de Seguridad Cibernética, dependiente del grado de clasificación de incidente;
12. Generar ciberinteligencia estratégica respecto de los servicios esenciales e infraestructura crítica del estado;
13. Coordinar con entidades y organismos públicos, privados e internacionales, para que de manera conjunta se desarrollen mecanismos de cooperación para la identificación de vulnerabilidades, amenazas y riesgos en el ciber espacio;
14. Promover procesos de formación y desarrollo de capacidades de los subsistemas, en ciberinteligencia, en el marco de sus atribuciones;
15. Apoyar en la planificación, ejecución, coordinación y participar en ejercicios para la ciberseguridad, ciberdefensa y ciberinteligencia a nivel nacional e internacional, conforme a la normativa correspondiente;
16. Coordinar la respuesta ante ataques y otros incidentes en el ciberespacio que puedan afectar a los subsistemas a su cargo; apoyar a las demás entidades públicas y privadas de interés estratégico para el estado y cooperar con las autoridades judiciales correspondientes;
17. Definir las acciones y recursos estratégicos, operativos y tácticos con las instituciones integrantes del Sistema Nacional de Seguridad Digital, a fin de contar con inteligencia y contrainteligencia estratégica.
18. Preparar y ejecutar la búsqueda, colección, interpretación y difusión de la inteligencia estratégica y prospectiva sobre amenazas, incidentes y riesgos para la toma de decisiones de las autoridades correspondientes, conforme al nivel de clasificación de la información;
19. Gestionar y promover, en coordinación con el ente rector de las relaciones exteriores y movilidad humana, la cooperación y asistencia técnica internacional, en materia de intercambio de información, y fortalecimiento de capacidades, conforme a los instrumentos internacionales suscritos por las entidades competentes del Estado ecuatoriano, con la finalidad de identificar, alertar y responder ante vulnerabilidades y amenazas que pongan en

riesgo la seguridad integral del Estado; y suscribir los acuerdos y convenios interinstitucionales en el ámbito de sus competencias

20. Participar en foros e iniciativas regionales y multilaterales sobre normativa internacional, medidas de fomento de la confianza y creación de capacidades en materia de seguridad digital;
21. Remitir, anualmente, o cuando lo amerite, al responsable del subsistema de ciberdiplomacia, los requerimientos de cooperación internacional; y,
22. Las demás establecidas en la Ley, el reglamento general de aplicación y las determinadas por el Comité Nacional de Seguridad Digital.

Sección Cuarta

SUBSISTEMA DE CIBERDIPLOMACIA

Artículo 51. Subsistema de Ciberdiplomacia.- El Subsistema de Ciberdiplomacia, estará conformado por el ente rector en materia de relaciones exteriores y movilidad humana, el ente rector en materia de comercio exterior, e integrará a los funcionarios públicos ante organizaciones internacionales u otras que el ente rector considere necesarias de conformidad con sus atribuciones y misión institucional.

El Subsistema de Ciberdiplomacia tendrá coordinación directa con el subsistema de ciberdefensa, el subsistema de ciberseguridad ciudadana y el subsistema de ciberinteligencia y articulará acciones con el Centro Nacional de Respuesta a Incidentes de Seguridad Digital, cuando se requiera la cooperación internacional para la detección oportuna y neutralización de amenazas, riesgos e incidentes; la prevención y combate al ciberdelito y la cibercriminalidad; la defensa de la soberanía y la seguridad integral; la política exterior y movilidad humana; y, la promoción del Ecuador en el exterior.

Artículo 52. Ente ejecutor de la política pública de ciberdiplomacia.- El ente rector en materia de relaciones exteriores y movilidad humana o el que haga sus veces, será responsable de la política pública en materia de ciberdiplomacia, para lo cual articulará sus actuaciones con el Comité Nacional de Seguridad Digital y las demás entidades y actores del Sistema Nacional de Seguridad Digital.

Artículo 53. Atribuciones y funciones del ente rector en materia de relaciones exteriores y movilidad humana . - Además de las funciones propias de la cartera de Estado y las funciones generales de las instituciones del Sistema Nacional de Seguridad Digital, el ente rector en materia de relaciones exteriores y movilidad humana tendrá las siguientes funciones y atribuciones:

1. Cumplir con las políticas públicas, estrategias, planes y acciones determinadas por el Comité Nacional Seguridad Digital y el ente rector del Sistema Nacional de Seguridad Digital;
2. Proteger los intereses nacionales y representar la posición nacional ante la comunidad internacional en materia de seguridad digital, de conformidad con las políticas determinadas por el Ente Rector del Sistema Nacional de Seguridad Digital, priorizando la seguridad digital internacional, los derechos humanos y la democracia;

3. Asesorar a las máximas autoridades de las Funciones del Estado respecto de los, mecanismos de cooperación internacional y asistencia técnica en materia de seguridad digital;
4. Definir e implementar planes, programas y proyectos para el mejoramiento de las capacidades de ciberdiplomacia, de conformidad con los lineamientos y directrices del Comité y ente rector del Sistema Nacional de Seguridad Digital;
5. Recopilar, procesar y analizar información con la finalidad proponer al Comité Nacional de Seguridad Digital, acciones, políticas o medidas en el marco de sus atribuciones para la reducción, repuesta y recuperación frente amenazas e incidentes en el ciberespacio;
6. Responder, en el marco de sus competencias, a los incidentes que puedan afectar al subsistema a su cargo, mediante acciones técnicas, oportunas y estratégicas, la recopilación de indicios o evidencias; y, reportar los resultados al Comité Nacional de Seguridad Digital;
7. Promover procesos de formación en seguridad digital y acceso a la verdad de los hechos en el marco de sus atribuciones;
8. Articular y fortalecer la participación del Ecuador en la cooperación bilateral, regional y multilateral para incrementar las capacidades estatales de reducción, respuesta y recuperación ante amenazas e incidentes que pueda poner en riesgo los intereses estratégicos del Estado;
9. Coordinar con las instituciones que forman parte del Sistema Nacional de Seguridad Digital para de manera conjunta desarrollar mecanismos de cooperación estratégica y operativa para proteger los intereses del Estado;
10. Promover y apoyar al resto de subsistemas para que participen en los mecanismos internacionales de cooperación, colaboración y asistencia, incluida la capacitación, ejercicios internacionales, intercambio de información, transferencia de conocimientos, alianzas estratégicas y acciones de respuesta, con otros países y organizaciones regionales e internacionales en materia de seguridad digital;
11. Insertar al Ecuador en las agendas regional y global, mediante el posicionamiento de asuntos digitales nacionales como un tema transversal para la consecución de los objetivos de desarrollo sostenible establecidos por la comunidad internacional;
12. Identificar, en coordinación con los demás subsistemas, las prioridades nacionales para la consecución de cooperación internacional en materia de seguridad digital;
13. Participar en foros e iniciativas regionales y multilaterales sobre normativa internacional, medidas de fomento de la confianza y creación de capacidades en materia de seguridad digital;
14. Gestionar y participar en esfuerzos internacionales de creación de capacidades y formación que contribuyan al resto de subsistemas a mejorar sus habilidades, conocimientos y capacidades técnicas en asuntos de prevención, identificación, mitigación, respuesta, resiliencia o defensa frente a amenazas e incidentes que provengan del ciber espacio;
15. Informar semestralmente, o cuando amerite, al Comité Nacional de Seguridad Digital sobre la cooperación internacional en materia de seguridad digital;
16. Desarrollar conocimientos y capacidad en ciberdiplomacia a fin de ser un miembro confiable y contribuyente a nivel regional y global en materia de seguridad digital;
17. Crear una unidad administrativa para asuntos exteriores digitales a cargo de una funcionaria o un funcionario de carrera de la primera o segunda categorías de acuerdo con la Ley Orgánica del Servicio Exterior; y,

18. Las demás establecidas en la Ley, el reglamento general de aplicación y las determinadas por el Comité Nacional de Seguridad Cibernética.

Sección Quinta

ENTIDADES AUXILIARES DEL SISTEMA NACIONAL DE SEGURIDAD DIGITAL

Artículo 54. Entidades auxiliares. – El Sistema Nacional de Seguridad Digital y sus subsistemas de Ciberdefensa, Ciberseguridad, Ciberinteligencia y Ciberdiplomacia, contarán con el apoyo técnico, asistencia y colaboración de las entidades auxiliares del Sistema Nacional de Seguridad Digital, a través de la coordinación establecida por el ministerio rector del Sistema.

Artículo 55. Atribuciones y funciones de la Agencia de Regulación y Control de las Telecomunicaciones.- Además de las atribuciones y funciones propias de su naturaleza, son atribuciones y funciones de la Agencia de Regulación y Control de Telecomunicaciones, las siguientes:

1. Cumplir con las políticas públicas, estrategias, planes y acciones determinadas por el Comité Nacional Seguridad Digital y el ente rector del Sistema Nacional de Seguridad Digital;
2. Generar informes, en el ámbito de sus competencias y remitirlos al ente rector y al Comité Nacional de Seguridad Digital;
3. Promover procesos de formación en seguridad digital y acceso a la verdad de los hechos en el marco de sus atribuciones;
4. Definir e implementar planes, programas y proyectos para el mejoramiento de las capacidades de seguridad digital en la entidad, de conformidad con los lineamientos y directrices del Comité y ente rector del Sistema Nacional de Seguridad Digital;
5. Proponer al Comité Nacional de Seguridad Digital, acciones, políticas o medidas en el marco de sus atribuciones para garantizar la seguridad digital;
6. Coordinar con todas las entidades a su cargo y ejecutar los procesos técnicos de vigilancia, auditoria, intervención y control en materia de seguridad cibernética;
7. Ejercer el control, regulación y sanción a los proveedores de servicios esenciales y operadores nacionales de infraestructura estratégica y crítica digital;
8. Las demás establecidas en la Ley, el reglamento general de aplicación y las determinadas por el Comité Nacional de Seguridad Digital.

Artículo 56. Atribuciones del Consejo de la Judicatura.- Además de las atribuciones y funciones propias de su naturaleza, el Consejo de la Judicatura tendrá las siguientes:

1. Cumplir con las políticas públicas, estrategias, planes y acciones determinadas por el Comité Nacional Seguridad Digital y el ente rector del Sistema Nacional de Seguridad digital;
2. Asegurar, en el marco de sus atribuciones y funciones constitucionales y legales, la observancia de los instrumentos internacionales en materia de seguridad digital;
3. Definir e implementar planes, programas y proyectos para el mejoramiento de las capacidades de seguridad digital en la Función Judicial, de conformidad con los lineamientos y directrices del Comité y ente rector del Sistema Nacional de Seguridad Digital;

4. Coordinar con las entidades competentes del Sistema Nacional de Seguridad Digital los procesos técnicos de vigilancia, auditoria, intervención y control en materia de seguridad Digital en las entidades de la Función Judicial;
5. Establecer un registro permanente sobre delitos informáticos y construir una estadística que permita tomar decisiones incorporando información de los entes que componen la Función Judicial;
6. Expedir los lineamientos y las directrices para la calificación de peritos para la realización de peritajes informáticos forenses y segmentarlos en especialidades, promoviendo que los peritos calificados cuenten con una certificación internacional;
7. Registrar e informar semestralmente de todos los procesos judiciales a escala nacional por delitos informáticos al Comité Nacional de Seguridad Digital; y, mediante un informe con los resultados de los procesos judiciales que se lleven a cabo en el sistema de justicia;
8. Promover procesos de formación en seguridad digital, seguridad sistémica y acceso a la verdad de los hechos en el marco de sus atribuciones;
9. Coordinar, a través de las Escuela de la Función Judicial y demás entidades de capacitación y especialización de la Defensoría Pública y la Fiscalía General del Estado, el desarrollo y ejecución de planes, programas y proyectos de capacitación a jueces, fiscales, peritos y demás funcionarios públicos de la Función Judicial en seguridad digital, investigación y combate a la ciberdelincuencia;
10. Establecer, en el ámbito de sus competencias, mecanismos de cooperación nacional e internacional para el fortalecimiento de las capacidades estatales para la prevención e investigación del ciberdelito y combate a la ciberdelincuencia, así como para garantizar el derecho de acceso a la verdad de los hechos;
11. Coordinar con todas las entidades a su cargo los procesos técnicos de vigilancia, intervención y control en materia de seguridad digital, seguridad sistémica y acceso a la verdad de los hechos;
12. Proponer al Comité Nacional de Seguridad Digital, acciones, políticas o medidas en el marco de sus atribuciones para garantizar ciberseguridad, seguridad sistémica y acceso a la verdad de los hechos; y,
13. Las demás establecidas en la Ley, el reglamento general de aplicación y las determinadas por el Comité Nacional de Seguridad Digital.

Artículo 57. Atribuciones y funciones de la Fiscalía General del Estado.- Además de las atribuciones y funciones propias de su naturaleza, la Fiscalía General del Estado tendrá las siguientes:

1. Cumplir con las políticas públicas, estrategias, planes y acciones determinadas por el Comité Nacional Seguridad Digital y el ente rector del Sistema Nacional de Seguridad Digita;
2. Definir e implementar planes, programas y proyectos para el mejoramiento de las capacidades de ciberseguridad, de conformidad con los lineamientos y directrices del Comité y ente rector del Sistema Nacional de Seguridad Digital;
3. Levantar, procesar y analizar información de carácter criminológico y proponer políticas y estrategias de prevención del ciberdelito y ciberdelincuencia en el ciberespacio;
4. Implementar mecanismos y estrategias para el análisis forense digital en los procesos de investigación de ciberdelitos;

5. Fortalecer la unidad especializada para la investigación y persecución de ciberdelitos y la ciberdelincuencia;
6. Promover la denuncia de los ciberdelitos y establecer los mecanismos necesarios para la denuncia e investigación de estos;
7. Elaborar estadísticas a nivel nacional relacionado con los delitos ocurridos en el ciberespacio;
8. Informar al Comité Nacional de Seguridad Digital las problemáticas e índices criminológicos de acuerdo con las denuncias presentas por delitos informáticos;
9. Registrar las denuncias a escala nacional por delitos informáticos y presentar reportes semestrales al ente rector del Sistema y del Comité Nacional de Seguridad Digital;
10. Promover procesos de formación en ciberseguridad, seguridad sistémica y acceso a la verdad de los hechos en el marco de sus atribuciones;
11. Solicitar y realizar técnicas especiales de investigación en los procesos por ciberdelitos y cibercrímenes;
12. Proponer al Comité Nacional de Seguridad Digital, acciones, políticas o medidas en el marco de sus atribuciones para garantizar ciberseguridad, seguridad sistémica y acceso a la verdad de los hechos;
13. Implementar, al través de la unidad respectiva y la escuela de la Función Judicial, procesos de capacitación a fiscales en seguridad digital;
14. Solicitar y brindar asistencia penal internacional en los procesos de investigación por ciberdelitos y cibercrímenes; y,
15. Las demás establecidas en el Código Orgánico Integral Penal, el reglamento a esta ley y las definidas por el Comité Nacional de Seguridad Digital.

Artículo 58. Atribuciones y funciones de las superintendencias como integrantes del Sistema Nacional de Seguridad Digital.- Las superintendencias, además de sus atribuciones y funciones propias, cumplirán las siguientes:

1. Cumplir con las políticas públicas, estrategias, planes y acciones determinadas por el Comité Nacional Seguridad Digital y el ente rector del Sistema Nacional de Seguridad Digital;
2. Definir e implementar planes, programas y proyectos para el mejoramiento de las capacidades de ciberseguridad, de conformidad con los lineamientos y directrices del Comité y ente rector del Sistema Nacional de Seguridad Digital;
3. Brindar colaboración expedita al Comité, el ente rector y a los subsistemas del Sistema Nacional de Seguridad Digital, cuando así les rea requerido;
4. Ejecutar en las áreas a su cargo procesos técnicos de vigilancia, auditoria, intervención y control en materia de ciberseguridad;
5. Proponer al Comité Nacional de Seguridad Digital, acciones, políticas o medidas en el marco de sus atribuciones para garantizar ciberseguridad, seguridad sistémica y acceso a la verdad de los hechos;
6. Promover procesos de formación en ciberseguridad, seguridad sistémica y acceso a la verdad de los hechos en el marco de sus atribuciones; y,
7. Las demás establecidas en la Ley, el reglamento general de aplicación y las determinadas por el Comité Nacional de Seguridad Digital.

Artículo 59. Atribuciones y funciones del Instituto Ecuatoriano de Normalización o su equivalente.- El Instituto Ecuatoriano de Normalización o su equivalente, además de las atribuciones y funciones de su propia naturaleza, tendrá las siguientes:

1. Cumplir con las políticas públicas, estrategias, planes y acciones determinadas por el Comité Nacional Seguridad Digital y el ente rector del Sistema Nacional de Seguridad Digital;
2. Definir e implementar planes, programas y proyectos para el mejoramiento de las capacidades de ciberseguridad, de conformidad con los lineamientos y directrices del Comité y ente rector del Sistema Nacional de Seguridad Digital;
3. Ejecutar en las áreas a su cargo procesos técnicos de vigilancia, auditoria, intervención y control en materia de seguridad digital;
4. Promulgar luego de un análisis técnico respectivo, las propuestas de normas, reglamentos técnicos, procedimientos de evaluación, procedimientos encaminados a garantizar seguridad digital;
5. Ejecutar acciones de normalización, reglamentación técnica y metrología encaminadas a garantizar seguridad digital;
6. Ejecutar en las áreas a su cargo procesos técnicos de auditoria, intervención y control en materia de seguridad digital, seguridad sistémica y acceso a la verdad de los hechos;
7. Proponer al Comité Nacional de Seguridad Cibernética, acciones, políticas o medidas en el marco de sus atribuciones para garantizar seguridad digital, seguridad sistémica y acceso a la verdad de los hechos;
8. Promover procesos de formación en seguridad digital, seguridad sistémica y acceso a la verdad de los hechos en el marco de sus atribuciones; y,
9. Las demás establecidas en la Ley, el reglamento general de aplicación y las determinadas por el Comité Nacional de Seguridad Digital.

Artículo 60. Responsables de seguridad digital.- El responsable de seguridad digital de las entidades que integran el Sistema, 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 digital; cumplirá los demás requisitos determinados en el reglamento general de aplicación de la presente ley; y, tendrá las siguientes funciones y atribuciones:

1. Cumplir con las acciones determinadas por el Comité Nacional Seguridad Digital;
2. Reportar, a través de las autoridades de la institución, los incidentes digitales que se hubiesen registrado, de acuerdo con las regulaciones y el protocolo definido por la entidad rectora del Sistema y precautelando los criterios de clasificación de la información;
3. Identificar y establecer protocolos, mecanismos, procedimientos, recursos u otros medios necesarios para asegurar la integridad, disponibilidad y confiabilidad de la información, evitando fugas de datos, adulteraciones o mutilaciones de la información digital;
4. Establecer, dirigir, orientar y coordinar la estrategia de seguridad digital de la institución de la que forma parte;
5. Determinar procedimientos para detectar, prevenir y analizar vulnerabilidades en la infraestructura tecnológica de su entidad;

6. Informar y reportar a sus superiores e instancias públicas pertinentes sobre cualquier amenaza, riesgo o incidente, de conformidad con los protocolos expedidos por la entidad rectora del Sistema;
7. Establecer procedimientos de sensibilización, capacitación y formación para el personal de la institución de la que forma parte, a fin de desarrollar una cultura de seguridad digital;
8. Denunciar a las autoridades judiciales pertinentes en caso de ciberdelitos y preservar los vestigios de tales incidentes y ponerlos a órdenes de la autoridad para realizar el peritaje forense informático correspondiente;
9. Alinear las estrategias y medidas de seguridad digital con las políticas, planes, programas, proyectos y normativa emitida por el Sistema Nacional de Seguridad Digital; y,
10. Las demás establecidas en la Ley, el reglamento general de aplicación y las determinadas por el Comité Nacional de Seguridad Digital.

CAPÍTULO VI

INSTRUMENTOS DEL SISTEMA NACIONAL DE SEGURIDAD DIGITAL Y MECANISMOS PARA EL ACCESO A LA VERDAD DE LOS HECHOS

Sección primera

INSTRUMENTOS DEL SISTEMA NACIONAL DE SEGURIDAD DIGITAL

Artículo 61. Instrumentos del Sistema Nacional de Seguridad Digital.- Son instrumentos para la reducción, respuesta y recuperación ante riesgos, amenazas e incidentes las siguientes:

1. Regulaciones y normas técnicas expedidas por las entidades de rectoría, regulación, coordinación, supervisión y control determinadas en la Ley Plan Nacional de reducción, respuesta y recuperación ante riegos, amenazas e incidentes digitales;
2. Plan Nacional de Seguridad Digital
3. Estrategia Nacional de Seguridad Digital
4. Planes sectoriales para la reducción, respuesta y recuperación ante riesgos, amenazas e incidentes digitales;
5. Planes institucionales para la reducción, respuesta y recuperación ante riesgos, amenazas e incidentes digitales;
6. Acreditaciones a operadores, proveedores y sistemas de información y comunicaciones;
7. Certificaciones
8. Red de puntos de contacto responsables de seguridad digital;
9. Plataformas de información y de capacitación en seguridad digital;
10. Ejercicios de seguridad digital;
11. Catálogo de incidentes;
12. Alertas automáticas de los sistemas
13. Otros creados o autorizados por el ente rector del Sistema Nacional de Seguridad Digital.

Artículo 62. Regulaciones y normas técnicas expedidas por las entidades de rectoría, regulación, coordinación, supervisión y control.- El ente rector del Sistema Nacional de

Seguridad Digital expedirá las normas técnicas para su regulación, coordinación, supervisión y control.

El ente rector de cada subsistema integrante del Sistema Nacional de Seguridad Digital se encargará de expedir la normativa secundaria correspondiente para regular a sus integrantes.

Artículo 63. Plan Nacional de Seguridad Digital.- El Plan Nacional de Seguridad Digital es el instrumento del Sistema Nacional de Seguridad Digital que determina la visión que el país tiene sobre la seguridad digital y resiliencia; determina los principios rectores, objetivos estratégicos de la política pública integral de ciberdefensa, ciberseguridad, ciberinteligencia y ciberdiplomacia; y, estará alineado al Plan Nacional de Desarrollo y al Plan Nacional de Seguridad Integral.

El Estado central y las respectivas entidades obligadas en la presente Ley, garantizarán desde sus planificaciones presupuestarias los recursos suficientes y oportunos para la ejecución de Plan Nacional de Seguridad Digital. El Plan estará diseñado para cuatro años con la especificación de metas anuales.

Artículo 64. Estrategia Nacional de Seguridad Digital.- Es el instrumento bianual aprobado por el Comité Nacional de Seguridad Digital que establece los ejes, pilares, líneas de acción, actividades u otros; y, los mecanismos de seguimiento y evaluación de su implementación, estableciendo un horizonte temporal para la aplicación del Plan Nacional de Seguridad Digital.

Artículo 65. Elaboración de la Estrategia de Seguridad Digital.- La Estrategia de Seguridad Digital será elaborada de manera bianual, por el ente rector del Sistema Nacional de Seguridad Digital, en coordinación con sus subsistemas mediante 5 fases:

1. Iniciación: En esta fase se determinará a la autoridad responsable del proyecto mediante designación del ente rector que será comunicada a la secretaría del Comité Nacional de Seguridad Digital al que propondrá los nombres de los candidatos para la conformación de un Comité Directivo encargado de apoyar a la autoridad responsable en la elaboración de la estrategia.
2. Inventario y análisis: En esta fase se recopilarán datos e información para evaluar el estado de situación actual, las principales vulnerabilidades y los posibles escenarios de gestión de riesgos digitales; programas locales de seguridad digital existentes, iniciativas internacionales, proyectos del sector privado, educación digital, iniciativas de investigación y desarrollo en materia de seguridad digital; las tasas de infección; perspectivas sobre las futuras tendencias y amenazas a la seguridad digital; entre otros datos que determine el ente rector del Sistema Nacional de Seguridad Digital a fin de identificar las principales debilidades y oportunidades en las capacidades de seguridad digital, respetando los niveles de clasificación de la información.
3. Producción: En esta fase se elaborará el texto de la estrategia con la participación de los principales interesados del sector público, el sector privado y la sociedad civil, a fin de definir ejes, pilares, líneas de acción, actividades u otros dentro de plazos concretos, proponer un marco de gobernanza, identificar a la entidad responsable de su evaluación y reforzar la preparación y gestión de crisis.
4. Ejecución: En esta fase se implementará la estrategia de manera estructurada, con los recursos financieros adecuados, determinando responsabilidades tanto para los actores

públicos como privados, de conformidad con el principio de cooperación, coordinación de esfuerzos y eficiencia en el uso de recursos.

5. Seguimiento y evaluación: En esta fase la Secretaría del Comité Nacional de Seguridad Digital, evaluará la estrategia mediante la verificación de la implementación. Se establecerán indicadores que permitan tener una valoración objetiva de cumplimiento de la misma, los que deberán ser específicos, cuantificables, viables, con responsables claramente identificados y plazos.

   La supervisión será permanente, de conformidad con los cronogramas y plazos determinados en la estrategia, a fin de que las partes involucradas puedan rendir cuentas del cumplimiento de sus responsabilidades y compromisos, así como para rectificar cualquier problema de ejecución. Se incluirá un análisis de riesgos en la evaluación que permita determinar cambios en la estrategia para asegurar sus resultados. El resultado de la evaluación constante en el respectivo informe de la Secretaría será presentado al Comité Nacional de Seguridad Digital, el que analizará la información a fin de tomar las decisiones correspondientes.

Artículo 66. Planes sectoriales para la reducción, respuesta y recuperación ante incidentes digitales .- Estos planes deben determinar las iniciativas específicas de cada esfera prioritaria que contribuirán a alcanzar objetivos definidos en la estrategia nacional de seguridad digital, en las diferentes esferas prioritarias identificadas en el Plan Nacional de Seguridad Digital. Además, debe establecer indicadores de cumplimiento para evaluar cada uno de los planes, programas, proyectos y políticas emitidas por los organismos nacionales y sectoriales.

Artículo 67. **Planes institucionales para la reducción, respuesta y recuperación ante incidentes digitales.-** Son los planes desarrollados por las instituciones públicas y privadas que tienen por objetivo la gestión de riesgos y la reducción, respuesta y recuperación ante incidentes al interior de la institución, cuya elaboración será anual, pudiendo actualizarse cuando las circunstancias lo requieran.

Artículo 68. Acreditaciones a operadores, proveedores y sistemas de información y comunicaciones.- El Instituto Ecuatoriano de Normalización o su equivalente acreditará a los prestadores de servicios esenciales y de infraestructuras críticas, empresas pública o privadas en el ámbito de seguridad digital de conformidad con los requisitos especificados en el Reglamento. La acreditación debe expedirse por un período máximo de cinco años y debe renovarse en las mismas condiciones, siempre y cuando se cumpla los requisitos. Los organismos nacionales de acreditación deben restringir, suspender o revocar la acreditación de un organismo cuando las condiciones de la acreditación no se cumplan, o hayan dejado de cumplirse.

Artículo 69. Certificaciones.- Las certificaciones son un instrumento del Sistema Nacional de Seguridad Digital que permite certificar a un producto, servicio o proceso en materia de seguridad digital. Los procedimientos se regularán mediante el reglamento que se promulgue para el efecto.

El cumplimiento de las certificaciones de seguridad digital, generarán acciones afirmativas y acceso preferencial a beneficios cuando corresponda. Las certificaciones están orientadas a promover las buenas prácticas de seguridad digital

Artículo 70. Red de puntos de contacto de responsables en seguridad digital.- La entidad rectora del Sistema Nacional de Seguridad Digital debe apoyar a las instituciones públicas y privadas, a fin de que logren una coordinación más estrecha y el intercambio de mejores prácticas, la creación de una red de puntos de contacto nacionales en materia de seguridad digital y el establecimiento de una plataforma de formación y enlace en caso de ataques.

Artículo 71. Plataformas de información y de capacitación en seguridad digital.- Con el fin de aumentar la resiliencia la Entidad Rectora del Sistema debe impulsar el desarrollo de conocimientos colectivos en el ámbito de la seguridad digital, ofreciendo asesoramiento, capacitación y orientaciones e intercambiando mejores prácticas. Con el fin de facilitar el acceso a una información mejor estructurada sobre los riesgos relacionados con la ciberseguridad y las posibles soluciones, la entidad rectora del Sistema de seguridad digital debe crear y mantener una o más plataformas de información y capacitación en seguridad digital, conforme al reglamento a esta ley.

Artículo 72. Ejercicios de Seguridad Digital.- Los ejercicios de seguridad digital es un instrumento del Sistema Nacional de Seguridad Digital encaminado a fortalecer sus capacidades para preservar la seguridad digital. Se realizarán de manera periódica conforme a las necesidades del sistema y se desarrollará según el reglamento que se apruebe pare el efecto.

Artículo 73. Catálogo de incidentes .- El catálogo es un repositorio de incidentes generados en el Sistema Nacional de Seguridad Digital, encaminado a provocar respuestas más eficientes e inmediatas, generar alertas automáticas, reconocer incidentes y amenazas, analizar científicamente el comportamiento de la seguridad digital, que sirve como mecanismo para la toma de decisiones.

Artículo 74. Alertas automáticas de los sistemas.- Los Centros de Respuesta a Incidentes de Seguridad Digital deberán alertar a sus usuarios que realicen actividades en o a través del ciberespacio, en los términos establecidos en la presente Ley, desarrollando sistemas de alertas automáticas de incidentes o amenazas u otros.

Las instituciones públicas y privadas deberán alertar sus usuarios que realicen actividades en o a través del ciberespacio, cuando sean posibles víctimas o hayan sido afectados por incidentes digitales en los términos establecidos en la presente Ley, desarrollando sistemas de alertas de amenazas conforme al reglamento general de aplicación de la presente ley.

Sección segunda

MECANISMOS PARA EL ACCESO A LA VERDAD DE LOS HECHOS

Artículo 75. Derecho a acceder a la verdad de los hechos.- Las personas tienen derecho a acceder a la verdad de los hechos, a través del Sistema Nacional de Seguridad Digital que se encuentra encaminado a que las víctimas de vulneraciones digitales puedan acceder a la información que permita el conocimiento del daño objetivo, la explicación técnica y motivada de los hechos, el

detalle de acciones y omisiones que se habrían detectado en los hechos, la generación de alertas automáticas de los sistemas; y, la trazabilidad y verificabilidad de la información.

Artículo 76. Mecanismos de acceso a la verdad de los hechos.- Todas las entidades y actores que realicen actividades en y a través del ciberespacio en los términos establecidos en la presente Ley deberán incorporar en sus plataformas y sistemas la posibilidad que las víctimas puedan solicitar acceso a la verdad de los hechos, respetando los niveles de clasificación de la información, de conformidad con lo determinado en el reglamento respectivo.

En las respuestas a las solicitudes se hará constar, al menos:

1. Especificación y detalle del daño objetivo en el caso de vulneración y del posible daño en el caso de amenaza;
2. Explicación y motivación de la alerta automática;
3. Explicación técnica y motivada de los hechos;
4. Detalle de acciones y omisiones que se habrían detectado en los hechos; y,
5. La trazabilidad y verificabilidad de la información.

Artículo 77. Buenas prácticas para promover el acceso a la verdad de los hechos.- En el desarrollo de las estrategias, planes, programas, proyectos y políticas públicas que implementen las entidades públicas que conforman en Sistema Nacional de Seguridad Digital se implementarán las buenas prácticas sugeridas a través de la adopción de estándares técnicos, nacionales o internacionales, con énfasis en gobierno digital; cultura de riesgo y resiliencia; digitalización de procesos; digitalización del 100% de los archivos institucionales; sistemas de identificación y seguimiento virtual de solicitudes y trámites ciudadanos; acceso en línea directo a información de ejecución presupuestaria institucional cuatrimestral o balances financieros anuales; mecanismos de participación y decisión para el cumplimiento de presupuestos participativos; espacio virtual de denuncias de actos de corrupción; mecanismos interactivos virtuales de formación que fomenten la cultura, historia y otros que determine el ente rector del Sistema Nacional de Seguridad Digital que permitan promover el acceso a la verdad de los hechos a través de la trazabilidad y otros medios tecnológicos correspondientes conforme al reglamento a general de aplicación de esta ley.

Sección tercera

FINANCIAMIENTO DEL SISTEMA NACIONAL DE SEGURIDAD DIGITAL

Artículo 78. Fondo para la Seguridad Digital, Seguridad Sistémica y Acceso a la Verdad de los Hechos.- Sin perjuicio de las asignaciones adicionales que tenga el Sistema Nacional de Seguridad Cibernética, su funcionamiento, las políticas públicas de ciberseguridad, seguridad sistémica y acceso a la verdad de los hechos, así como la aplicación de los instrumentos del Sistema se financiarán mediante el Fondo para la Ciberseguridad de conformidad con el Reglamento General de aplicación de esta ley.

DISPOSICIONES GENERALES

PRIMERA. – **Financiamiento para la ejecución de planes, programas y proyectos.-** En los casos en los que corresponda, la ejecución de planes, programas, proyectos y las acciones conducentes a la materialización y garantía plena de las disposiciones contempladas en la presente Ley se financiarán mediante la programación presupuestaria de cada entidad obligada o responsable.

SEGUNDA.- Control democrático.- La entidad rectora del Sistema Nacional de Seguridad Cibernética, en sesión reservada semestral, rendirá cuentas de forma ante la Asamblea Nacional a través de la Comisión responsable de la temática de seguridad.

DISPOSICIONES REFORMATORIAS

PRIMERA.- Agréguese en el Código Orgánico Monetario y Financiero en su artículo 14.1 Funciones. Para el desempeño de sus funciones, la Junta de Política y Regulación Financiera tiene que cumplir los siguientes deberes y ejercer las siguientes facultades: (...)

15. Establecer, en el marco de sus competencias, cualquier medida que coadyuve a : (...)

e. Prevenir y erradicar malas prácticas o delitos informáticos en la operación y funcionamiento de las entidades financieras, seguros y servicios de atención integral de salud prepagada, mediante la implementación de buenas prácticas de seguridad digital, considerando los estándares nacionales e internaciones y el avance tecnológico.

SEGUNDA.- Agréguese en el Código Orgánico Monetario y Financiero en su artículo 62 Funciones. A Superintendencia de Bancos tiene las siguientes funciones:

9. Exigir que las entidades controladas presenten y adopten las correspondientes medidas correctivas y de saneamiento, en especial en delitos informáticos y tecnológicos e imponer sanciones por incumplimiento en políticas de seguridad digital;

TERCERA.- Agréguese en la Ley Orgánica de la Economía Popular y Solidaria, en el artículo 147 Atribuciones. La Superintendencia tendrá las siguientes atribuciones:

e. Exigir que las entidades controladas presenten y adopten las correspondientes medidas correctivas y de saneamiento, en especial en delitos e incidentes informáticos y tecnológicos e imponer sanciones por incumplimiento en políticas de seguridad digital (...)

i. Las demás previstas en la Ley y su Reglamento.

CUARTA.- Agréguese en la Ley Orgánica de Datos Personales, en su artículo Art. 76.- Funciones atribuciones y facultades. La Autoridad de Protección de Datos Personales es el órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la Protección de sus datos personales, y de realizar todas las acciones necesarias para que se respeten los principios, derechos garantías y

procedimientos previstos en la presente Ley y en su reglamento de aplicación, para lo cual le corresponde las siguientes funciones, atribuciones y facultades;

18) Entregar un informe trimestral de riesgos, incidentes y ataques informáticos registrados en relación a la protección de datos, al ente rector del Sistema Nacional de Seguridad Digital, para su análisis y decisión en la generación de políticas públicas.

19) Las demás atribuciones establecidas en la normativa vigente.

DISPOSICIONES TRANSITORIAS

PRIMERA.- El Presidente de la República del Ecuador, en un plazo de 120 día, a partir de la publicación de la presente ley en el Registro Oficial, expedirá el reglamento general de aplicación.

SEGUNDA: Las entidades, organismos y actores del Sistema Nacional de Seguridad Digital adecuarán su normativa secundaria, estrategias, planes y políticas públicas a la presente Ley en un plazo máximo de 180 días contados desde la entrada en vigor.

DISPOSICIÓN FINAL.- Esta ley entrará en vigor a partir de su publicación en el Registro Oficial.

Dado y suscrito en la sede de la Asamblea Nacional, ubicada en el Distrito Metropolitano de

Quito, provincia de Pichincha a los...

12. CERTIFICACIÓN DE LA SECRETARIA O SECRETARIO RELATOR DE LOS DÍAS EN QUE FUE DEBATIDO EL PROYECTO DE LEY, ACUERDO, RESOLUCIÓN O DEMÁS ACTOS LEGISLATIVOS, SEGÚN CORRESPONDA

RAZÓN: Siento como tal, que el Proyecto de Ley Orgánica de Seguridad Digital fue debatido y aprobado en el Pleno de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral en sesión No. 209, del día 22 de marzo de 2023.-

Quito, 22 de marzo de 2023.- Lo certifico.

Firmado electrónicamente por:
JAVIER ANDRES BORJA ORTIZ

Abg. Javier Andrés Borja
Secretario Relator de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral

13. DETALLE DE ANEXOS

ANEXO 1: Oficio Nro. CIES-CIES-0108-2022-OF
ANEXO 2: Observaciones Ley de Seguridad Digital:
ANEXO 3: Observaciones Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa, Ciberinteligencia
ANEXO 4: Observaciones Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos
ANEXO 5: Oficio Nro. CIES-CIES-0195-2022-OF
ANEXO 6: Propuesta de Unificación CIES: Ley de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia
ANEXO 7: Oficio Nro. MDN-MDN-2022-0982-OF
ANEXO 8: Matriz de Observaciones a los Proyectos de Seguridad Digital, MIDENA
ANEXO 9: REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación punto (2). Disponible en: Disponible en: Reglamento (UE) 2019/ del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 (Reglamento sobre la Ciberseguridad) (europa.eu)

Link de anexos:
https://drive.google.com/drive/folders/1dVQzrWSN40cSntYgMiCN3nofqdpKFDNW?usp=share_link