REPÚBLICA DEL ECUADOR

Asamblea Nacional

Acta 922-A

28 DE MAYO DE 2024

SUMARIO:

REPÚBLICA DEL ECUADOR

Asamblea Nacional

Acta 922-A

ÍNDICE:

REPÚBLICA DEL ECUADOR

Asamblea Nacional

Acta 922-A

ANEXOS:

1. **Convocatoria y orden del día.**

2. **Conocer y resolver respecto del informe para segundo debate del Proyecto de Ley Orgánica de Seguridad Digital.**

   2.1. **Memorando No. AN-CSIS-2024-0179-M. Quito, D.M, 02 de mayo de 2024, suscrito por el magíster Marco Danilo Jirón Paredes, secretario relator de la Comisión de Soberanía, Integración y Seguridad Integral; remitiendo informe de la comisión.**

3. **Resumen Ejecutivo de la Sesión del Pleno de la Asamblea Nacional.**

4. **Listado de Asambleístas asistentes a la sesión del Pleno de la Asamblea Nacional.**

REPÚBLICA DEL ECUADOR

Asamblea Nacional

Acta 922-A

En la sala de sesiones de la Asamblea Nacional, ubicada en la ciudad de Quito, Distrito Metropolitano, a las doce horas cuarenta y dos minutos del día veintiocho de mayo del año dos mil veinticuatro, se instala la sesión de la Asamblea Nacional, dirigida por su presidente, asambleísta Henry Kronfle Kozhaya. ----------

En la Secretaría actúa la abogada María Soledad Rocha Díaz, prosecretaria general de la Asamblea Nacional. ----------

EL SEÑOR PRESIDENTE. Señores y señoras asambleístas, buenas tardes nuevamente. Señorita prosecretaria, verifique el cuórum para instalar la continuación de la Sesión novecientos veintidós. ----------

I

LA SEÑORA SECRETARIA. Con su autorización, señor presidente. Señoras y señores asambleístas, por favor, registrar su asistencia en las curules electrónicas. De existir alguna novedad, informar a esta Secretaría y a cada uno de los técnicos asignados. Gracias. ----------

EL SEÑOR PRESIDENTE. Señores asambleístas, les ruego, por favor, registrarse. Bastantes asambleístas en el Pleno que aún no se registran. Por favor, registrarse lo antes posible. Cierre el registro, por favor. -------

LA SEÑORA SECRETARIA. Me permito informar, señor presidente, que contamos con ciento veintiún asambleístas registrados en la sesión. Contamos con el cuórum legal. ----------

II

EL SEÑOR PRESIDENTE. Se instala la continuación de la Sesión

número novecientos veintidós. Señorita prosecretaria, dé lectura a la convocatoria. ----------

III

LA SEÑORA SECRETARIA. Con su autorización, señor presidente. "Convocatoria. Por disposición del ingeniero Henry Kronfle Kozhaya, presidente de la Asamblea Nacional, de conformidad con el artículo 12 numeral 3 de la Ley Orgánica de la Función Legislativa, se convoca a las y los asambleístas a la continuación de la Sesión Nro. 922 del Pleno de la Asamblea Nacional, a realizarse el día martes 28 de mayo de 2024, a las 11h30, en la sede de la Función Legislativa, ubicada en la Avenida 6 de Diciembre y Piedrahita en el cantón Quito, provincia de Pichincha, con el objeto de tratar el siguiente orden del día aprobado: Conocer y resolver respecto del informe para segundo debate del Proyecto de Ley Orgánica de Seguridad Digital". Hasta ahí la lectura de la convocatoria, señor presidente. ----------

EL SEÑOR PRESIDENTE. Gracias. Siguiente punto del orden del día, señorita prosecretaria. ----------

IV

LA SEÑORA SECRETARIA. "Conocer y resolver respecto del informe para segundo debate del Proyecto de Ley Orgánica de Seguridad Digital". ----------

EL SEÑOR PRESIDENTE. Dé lectura del informe en su parte resolutiva, por favor. ----------

Acta 922-A

LA SEÑORA SECRETARIA. Con su autorización, señor presidente. "Memorando Nro. AN-CSIS-2024-0179-M. Quito, D.M., 02 de mayo de 2024. Para: Señor magíster Henry Fabián Kronfle Kozhaya, presidente de la Asamblea Nacional. Asunto: Se remite el informe para segundo debate de la Ley Orgánica de Seguridad Digital. De mi consideración: Por disposición de la presidente de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, asambleísta Inés Alarcón, amparado en el artículo 61 de la Ley Orgánica de la Función Legislativa, y del artículo 32 del Reglamento de Comisiones Especializadas Permanentes y Ocasionales, tengo a bien remitir el informe para segundo debate del Proyecto de Ley Orgánica de Seguridad Digital, aprobado el 01 de mayo de 2024, de abril de 2024, a fin de que se continúe con el trámite respectivo en el Pleno de la Asamblea Nacional. El Asambleísta ponente del proyecto es la asambleísta Inés Alarcón. La votación realizada en la Sesión ordinaria Nro. 37 es el siguiente: Afirmativo: ocho (8). Negativo: cero (0). Abstención: cero (0). Asambleístas ausentes: uno (1). Al ser entregado el presente memorando de manera física, se deja constancia de adjunto al mismo en impreso el informe detallado en 210 fojas útiles. Con sentimientos de distinguida consideración. Atentamente, magíster Marco Danilo Jirón Paredes, secretario relator". Me permito leer la parte pertinente y resolutiva del informe: "1. Objeto del informe. El presente informe tiene como objeto poner en conocimiento del Pleno de la Asamblea Nacional el texto del informe para segundo debate del Proyecto de Ley Orgánica de Seguridad Digital, que unifica tres iniciativas que han sido procesadas para su tratamiento por parte de la Comisión Permanente de Soberanía, Integración y Seguridad Integral, en 23 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, ciberseguridad, ciberinteligencia y ciberdiplomacia. 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 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 periodo 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 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 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 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 exasambleísta Juan Carlos Yar y, en la misma sesión, aprobó la moción para su unificación al Código Orgánico de Seguridad Integral. En Sesión 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 presenten 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 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 Orgánico de Seguridad del Estado. 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 Ciberseguridad, 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 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 Nro. 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 a 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 coronel (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 señora Vianna di María 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 Nro. 132, de 15 de junio de 2022, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, 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 Nro. 133 de 15 de junio de 2022, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, 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 contraparte técnica de la comisión en la elaboración del texto para primer debate de la normativa legal, proporcionando 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 2002, 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 al 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 de los proyectos de ley sobre ciberseguridad. En Sesión ordinaria Nro. 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 derecho 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 Nro. 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 del 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 magíster 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 María 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 al 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 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 del 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. En Sesión Nro. 002 del nuevo periodo legislativo, de 30 de noviembre de 2023, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral puso en conocimiento el debate y aprobación de la propuesta de plan de trabajo de la Comisión Especializada de Soberanía, Integración y Seguridad Integral para el período 2023-2025. En Sesión Nro. 004, de 13 de diciembre de 2023, se puso en conocimiento los plazos y estado actual del Proyecto de Ley Orgánica de Seguridad Digital a la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral. La presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral solicitó aportes y observaciones al Proyecto de Ley Orgánica de Seguridad Digital a las siguientes autoridades: Mediante Oficio Nro. AN-CSIS-2024-0055-O, de 21 de diciembre de 2023, al señor Gian Carlo Loffredo Rendón, ministro de Defensa Nacional. Mediante Oficio Nro. AN-CSIS-2023-0256-O, de 21 de diciembre de 2023, a la señora Mónica Rosa Irene Palencia Núñez, ministra del Ministerio del Interior (E). Mediante Oficio Nro. AN-CSIS-2023-0257-O, de 21 de diciembre de 2023, a la señora María Gabriela Sommerfeld Rosero,

canciller del Ministerio de Relaciones Exteriores y Movilidad Humana. Mediante Oficio Nro. AN-CSIS-2023-0258-O, de 21 de diciembre de 2023, al señor abogado William Edwar Birkett Mortola, director general de Aviación Civil. Mediante Oficio Nro. AN-CSIS-2023-0259-O, de 21 de diciembre de 2023, a la señora doctora Lady Diana Salazar Méndez, fiscal general del Estado. Mediante Oficio Nro. AN-CSIS-2023-0260-O, de 21 de enero de 2023, al señor ingeniero Roberto Xavier Luque Nuques, ministro de Transporte y Obras Públicas. Mediante Oficio Nro. AN-CSIS-2023-0261-O, de 21 de enero de 2023, al señor doctor Iván Patricio Saquicela Rodas, presidente de la Corte Nacional de Justicia. Mediante Oficio Nro. AN-CSIS-2023-0262-O, de 21 de diciembre de 2023, al abogado Juan Carlos Larrea Valencia, procurador general del Estado. Mediante Oficio Nro. AN-CSIS-2023-0263-O, de 21 de diciembre de 2023, al señor César Antonio Martin Moreno, ministerio de Telecomunicaciones. Mediante Oficio Nro. AN-CSIS-2023-0264-O, de 21 de diciembre de 2023, a la señora Mónica Rosa Irene Palencia Núñez, ministra de Gobierno. Mediante Oficio Nro. AN-CSIS-2023-0265-O, de 21 de diciembre de 2023, al señor coronel Fausto Antonio Cobo Montalvo, director general del Centro de Inteligencia Estratégica (CIES). Mediante Oficio Nro. AN-CSIS-2023-0266-O, de 21 de diciembre de 2023, al señor magíster Luis Eduardo Zaldumbide López, director general de Servicio Nacional Atención Integral a Personas Adultas Privadas Libertad (SNAI). Mediante Oficio Nro. AN-CSIS-2023-0267-O, de 21 de diciembre de 2023, al señor magíster Ángel Rodrigo Rosero Gómez, director general del Servicio Nacional de Gestión de Riesgos y Emergencias. Mediante Oficio Nro. AN-CSIS-2023-0269-O, de 21 de diciembre de 2023, al señor magíster Daniel Augusto Arboleda Villacreses, director nacional de Registros Públicos. Mediante Oficio Nro. AN-CSIS-2023-0270-O, de 21 de diciembre de 2023, al señor

máster Damián Alberto Larco Guamán, director general del Servicio de Rentas Internas. Mediante Oficio Nro. AN-CSIS-2023-0271-O, de 21 de diciembre de 2023, al señor magíster Bolívar Wladimir Tello Astudillo, director general del ECU-911. Mediante Oficio Nro. AN-CSIS-2023-0273-O, de 21 de diciembre de 2023, a la señora magíster María Gabriela Ochoa Ochoa, directora general del Servicio Nacional de Aduanas. Mediante Oficio Nro. AN-CSIS-2023-0274-O, de 21 de diciembre de 2023, a la señora magíster Silvia Pamela Mendieta Molina, directora ejecutiva de la Agencia Nacional de Tránsito. Mediante Oficio Nro. AN-CSIS-2023-0275-O, de 21 de diciembre de 2023, al ingeniero comercial Marco Giovanni López Narváez, superintendente de Compañías, Valores y Seguros. Mediante Oficio Nro. AN-CSIS-2023-0276-O, de 21 de diciembre de 2023, a la señora magíster Antonieta Guadalupe Cabezas Enríquez, superintendente de Bancos. Mediante Oficio Nro. AN-CSIS-2023-0277-O, de 21 de diciembre de 2023, al doctor Danilo Ivanob Sylva Pazmiño, superintendente de Control del Poder de Mercado. Mediante Oficio Nro. AN-CSIS-2023-0278-O, de 21 de diciembre de 2023, a la señora doctora Sofía Margarita Hernández Naranjo, superintendente de Economía Popular y Solidaria. Mediante Oficio Nro. AN-CSIS-2023-0279-O, de 21 de diciembre de 2023, al señor ingeniero Pablo Ramiro Iglesias Paladines, superintendente de Ordenamiento Territorial, Uso y Gestión del Suelo. Mediante Oficio Nro. AN-CSIS-2023-0280-O, de 21 de diciembre de 2023, a la señora magíster María de Lourdes Cuesta Orellana, gerente general CNT. Mediante Oficio Nro. AN-CSIS-2023-0281-O, de 21 de diciembre de 2023, a la doctora Paola Verenice Pabón Caranqui, presidenta del Consorcio de Gobiernos Autónomos Provinciales del Ecuador (Congope). Mediante Oficio Nro. AN-CSIS-2023-0282-O, de 21 de diciembre de 2023, al señor William Patricio Maldonado Jiménez, presidente de la

Asociación Municipalidades Ecuatorianas (AME). Mediante Oficio Nro. AN-CSIS-2024-0011-SR, de 21 de enero de 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral solicitó aportes y observaciones al Proyecto de Ley Orgánica de Seguridad Digital, al señor magíster Javier Andrés Borja, experto en seguridad digital. Mediante Oficio Nro. AN-CSIS-2024-0058-O, de 23 de enero de 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral solicitó aportes y observaciones al Proyecto de Ley Orgánica de Seguridad Digital, al señor Arturo David Félix Wong, secretario general de la Administración Pública de la Presidencia de la República. Mediante Oficio Nro. AN-CSIS-2024-0018-SR, de 25 de enero de 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral solicitó aportes y observaciones al Proyecto de Ley Orgánica de Seguridad Digital, al señor Juan Carlos Crespo Cruz de Grupo Radical. Mediante Oficio Nro. AN-CSIS-2024-0019-SR, de 05 de febrero de 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral solicitó aportes y observaciones al Proyecto de Ley Orgánica de Seguridad Digital, al señor Jorge Cástulo Guerrón, experto en seguridad digital, así como se realizó la invitación a participar en la comisión para presentar sus observaciones en la sesión de comisión del 07 de febrero de 2024. La presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibe las observaciones oficialmente por las diferentes instituciones públicas, expertos y académicos, respecto al Proyecto de Ley Orgánica de Seguridad Digital: Mediante Oficio Nro. NAC-DNJOGEC24-00000004, de 03 de enero 2024, la comisión recibe las observaciones del economista Damián Alberto Larco Guamán, director general de Servicio de Rentas Internas.

Acta 922-A

Mediante Oficio Nro. SCVS-DSC-2024-00000552-O, de 03 de enero 2024, la comisión recibe las observaciones del señor ingeniero Marco López Narváez, superintendente de Compañías, valores y seguros. Mediante correo electrónico oficial Zimbra de la Asamblea Nacional, de 03 de enero de 2024, se recibió las observaciones realizadas por el ingeniero Luis Enríquez, experto en ciberseguridad. Mediante Oficio Nro. SEPS-SGD-2024-00646-OF, de 09 de enero 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital de la señora Sofía Margarita Hernández Naranjo, superintendente de Economía Popular y Solidaria. Mediante Oficio Nro. MDG-MDG-2024-0035-O, de 09 de enero 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital de la doctora Mónica Rosa Irene Palencia Núñez, ministra de Gobierno. La presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones oficialmente por las diferentes instituciones públicas, expertos y académicos, respecto al Proyecto de Ley Orgánica de Seguridad Digital: Mediante Oficio Nro. DE-2024-020-O, del 10 de enero 2024, la comisión recibe las observaciones de la doctora Ana María Larrea, directora ejecutiva del Consorcio de Gobiernos Autónomos Provinciales del Ecuador (Congope). Mediante Oficio SCE-2024-008, de 10 de enero 2024, la comisión recibe las observaciones del doctor Danilo Ivanob Sylva Pazmiño, superintendente de Competencia Económica, en el cual adjunta los memorandos SCE-IGG-INTIC-2024-010 y SCE-DS-INJ-2024-009, que contienen las observaciones pertinentes. Mediante Oficio Nro. SB-IG-2024-0008-O, de 10 de enero 2024, la comisión recibe las

observaciones de un informe técnico jurídico Nro. SB-INJ-2024-0039-M, por parte de la señora magíster María Belén Mora Villón, intendente general (S). Mediante Oficio Nro. SGR-SGR-2024-0036-O, de 10 de enero 2024, la comisión recibe las observaciones del señor magíster en ingeniería Jorge Raúl Carrillo Tutiven, secretario de Gestión de Riesgos. Mediante Oficio Nro. MREMH-MREMH-2024-0030-OF, de 10 de enero de 2024, la comisión recibe las observaciones de la señora María Gabriela Sommerfeld Rosero, ministra de Relaciones Exteriores y Movilidad Humana. Mediante Oficio Nro. SENAE-SENAE-2024-0016-OF, de 11 de enero 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, de la magíster María Gabriela Ochoa Ochoa, directora general del Servicio Nacional de Aduanas del Ecuador. Mediante Oficio Nro. MTOP-DVIT-24-27-OF, de 12 de enero de 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital del ingeniero Alex Raúl Villacrés Sánchez, viceministro de la Infraestructura del Transporte y Obras Públicas. Mediante Oficio Nro. MDN-MDN-2024-0114-OF, de 15 de enero 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital del señor Gian Carlo Loffredo Rendón, ministro de Defensa. Mediante Memorando Nro. AN-CSIS-2024-0027-M, de 16 de enero de 2024, el magíster Marco Jirón, secretario relator, solicita la autorización de la prórroga de noventa días que establece la Ley Orgánica de la Función Legislativa para la presentación del informe para segundo debate de la Ley Orgánica de Seguridad Digital, al señor magíster Henry Fabián Kronfle,

presidente de la Asamblea Nacional. Mediante Memorando Nro. AN-SG-2024-0204-M, de 17 de enero de 2024, la abogada María Soledad Rocha Díaz, prosecretaria general de la Asamblea Nacional, remite a la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral de la Asamblea Nacional, al señor magíster Marco Danilo Jirón Paredes la respuesta al memorando Nro. AN-CSIS-2024-0027-M, solicitud de prórroga para presentación del informe para segundo debate de la Ley Orgánica de Seguridad Digital; misma que fue autorizada una prórroga de noventa (90) días para entregar el mencionado informe. La presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, invitó a varias instituciones públicas, expertos y la academia, para presentar las observaciones y aportes respecto del Proyecto de Ley Orgánica de Seguridad Digital en diferentes sesiones generales de comisión: Mediante Oficio Nro. AN-CSIS-2024-0051-O, de 23 de enero de 2024, se invitó y solicitó aportes y observaciones al señor Efrén Ernesto Guerrero Salgado, docente de la Pontificia Universidad Católica del Ecuador. Mediante Oficio Nro. AN-CSIS-2024-0016-SR, de 23 de enero de 2024, se invitó y solicitó aportes y observaciones al señor Diego Álvarez, experto en seguridad digital. Mediante Oficio Nro. AN-CSIS-2024-0052-O, de 23 de enero de 2024, invitó a participar a los delegados del Ministerio de Gobierno. Mediante Oficio Nro. AN-CSIS-2024-0053-O, de 23 de enero de 2024, invitó a un delegado del Ministerio del Interior. Mediante Oficio Nro. AN-CSIS-2024-0054-O, de 23 de enero de 2024, invitó a un delegado del Ministerio de Defensa Nacional. Mediante Oficio Nro. AN-CSIS-2024-0055-O, de 23 de enero de 2024, invitó a un delegado del Ministerio de Telecomunicaciones. Mediante Oficio Nro. AN-CSIS-2024-0056-O, de 23 de enero de 2024, invitó a un delegado del Servicio Nacional de Atención Integral a Personas Adultas Privadas

de la Libertad (SNAI). Mediante Oficio Nro. AN-CSIS-2024-0061-O, de 23 de enero de 2024, invitó a un delegado del Servicio de Rentas Internas. Mediante Oficio Nro. AN-CSIS-2024-0062-O, de 23 de enero de 2024, invitó a un delegado de la Fiscalía General del Estado. Mediante Oficio Nro. AN-CSIS-2024-0063-O, de 23 de enero de 2024, invitó a un delegado del Servicio Nacional de Aduanas. Mediante Oficio Nro. AN-CSIS-2024-0064-O, de 23 de enero de 2024, invitó a un delegado de la Agencia de Regulación y Control de Telecomunicaciones. Mediante Oficio Nro. AN-CSIS-2024-0065-O, de 23 de enero de 2024, invitó a un delegado de la Procuraduría General del Estado. Mediante Oficio Nro. AN-CSIS-2024-0066-O, de 23 de enero de 2024, invitó a un delegado de la Unidad de Análisis Financiero y Económico (UAFE). En Sesión Nro. 017, realizada el 23 de enero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibió al Ministerio de Telecomunicaciones y de la Sociedad de la Información, Ministerio de Defensa, Ministerio de Gobierno, Ministerio del Interior, Centro de Inteligencia Estratégica, Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y Adolescentes Infractores; a los expertos Kevin Palacios, Efrén Guerrero Salgado y Diego Álvarez, para que expongan sus observaciones y análisis al Proyecto de Ley Orgánica de Seguridad Digital. En Sesión Nro. 019, realizada el 24 de enero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibió a la Procuraduría General del Estado, Agencia de Regulación y Control de las Telecomunicaciones, Fiscalía General del Estado, Unidad de Análisis Financiero del Ecuador, Centro de Inteligencia Estratégica, Servicio de Rentas Internas, Servicio Nacional de Aduanas del Ecuador y al abogado Javier Andrés Borja, experto en seguridad digital, para que expongan sus observaciones y

análisis al Proyecto de Ley Orgánica de Seguridad Digital. Mediante Oficio Nro. 05315, de 24 de enero de 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital del abogado Juan Carlos Larrea Valencia, procurador General del Estado. Mediante Oficio Nro. SNAI-SNAI-2024-0111-O, de 24 de enero 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital del general de brigadas (SP) Luis Eduardo Zaldumbide López, director general del Servicio Nacional de Atención Integral a Personas Adultas de la Libertad y a Adolescentes Infractores. Mediante correo electrónico oficial Zimbra de la Asamblea Nacional, de 24 de enero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por el señor Efrén Guerrero Salgado, profesor titular de la facultad de jurisprudencia de la Pontificia Universidad Católica del Ecuador. Mediante Oficio Nro. SIS-SIS-2024-0072-OF, de 25 de enero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por el magíster Bolívar Wladimir Tello Astudillo, director general del ECU-911. La presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, invitó a varias instituciones públicas, expertos y la academia, para presentar las observaciones y aportes respecto del Proyecto de Ley Orgánica de Seguridad Digital en diferentes sesiones generales de comisión: Mediante Oficio Nro. AN-CSIS-2024-0068-O, de 25 de enero de 2024, invitó y solicitó aportes y observaciones al señor

Acta 922-A

Alex Martínez Ramos, presidente de la Asociación Ecuatoriana de Ciberseguridad (AECI). Mediante Oficio Nro. AN-CSIS-2024-0070-O, de 25 de enero de 2024, invitó a un delegado del ECU-911. Mediante Oficio Nro. AN-CSIS-2024-0071-O, de 25 de enero de 2024, invitó a un delegado de la Dirección Nacional de Registro de Datos Públicos. Mediante Oficio Nro. AN-CSIS-2024-0072-O, de 25 de enero de 2024, invitó a un delegado del Consorcio de Gobiernos Autónomos Provinciales del Ecuador (Congope). Mediante Oficio Nro. AN-CSIS-2024-0073-O, de 25 de enero de 2024, invitó a un delegado de la Asociación de Municipalidades Ecuatorianas (AME)–Regional 6. Mediante Oficio Nro. AN-CSIS-2024-0018-SR, de 25 de enero de 2024, se invita a un delegado de Grupo Radical. En Sesión Nro. 021, realizada el 25 de enero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibió al Centro de Inteligencia Estratégica (CIES), Secretaría Nacional de Seguridad Pública y del Estado, Servicio Integrado de Seguridad (Ecu-911), Dirección Nacional de Registros Públicos (Dinardap), Consorcio de Gobiernos Autónomos Provinciales del Ecuador (Congope), Asociación de Municipalidades del Ecuador (AME), Consejo Nacional de Gobiernos Parroquiales Rurales del Ecuador (Conagopare), Servicio Nacional de Aduanas del Ecuador; a los expertos magíster Alex Martínez, señor Polo Fabián y señor Juan Carlos Crespo, para que expongan sus observaciones y análisis al Proyecto de Ley Orgánica de Seguridad Digital. Mediante correo electrónico oficial Zimbra de la Asamblea Nacional, de 28 de enero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital del señor Fabian Íñiguez, asesor de Grupo Radical. Mediante Oficio Nro. AECI-2024-0129-OR-001, de 29 de enero del 2024, la Comisión

Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, por el señor Alex Martínez Ramos, magíster, presidente de la Asociación Ecuatoriana de Ciberseguridad (AECI). Mediante Oficio Nro. CIES-CIES-2024-0021-OF, de 29 de enero del 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital del señor Michele Sensi Contugi Ycaza, director general del Centro de Inteligencia Estratégica (CIES). Mediante Oficio Nro. DGAC-DGAC-2024-0302-O, de 02 de febrero de 2024, la comisión recibe las observaciones del ingeniero Oswaldo Roberto Ramos Ferrusola, director general de Aviación Civil (E), en el cual consta el Memorando Nro. DGAC-DASJ-2024-0067-M, con fecha 24 de enero de 2024, con las observaciones realizadas por la magíster Rosa Herminia Álvarez Rivera, directora de Asesoría Jurídica. En Sesión Nro. 022, realizada el 06 de febrero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibió a Víctor Andrés Quishpe de la Unión Nacional de Educadores; Jorge Cástulo Guerrón, experto en Seguridad Digital; Diego Urbina, gerente de Región Sur de Amazon Web Services; y Arturo Cabaña, experto en seguridad digital, para que expongan sus observaciones y análisis al Proyecto de Ley Orgánica de Seguridad Digital. Mediante correo electrónico oficial Zimbra de la Asamblea Nacional, de 06 de febrero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, por el señor Diego Álvarez, country manager Ecuador, Niubox. Mediante correo electrónico oficial Zimbra de la Asamblea Nacional, de 07 de febrero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad

Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por el señor Jorge Guerrón, experto en seguridad digital. Mediante correo electrónico oficial Zimbra de la Asamblea Nacional, de 08 de febrero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital del economista Alan Sierra Nieto, director general de la Unidad de Análisis Financiero y Económico (UAFE). Mediante correo electrónico oficial Zimbra de la Asamblea Nacional, de 08 de febrero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por el señor Diego Urbina, gerente de Región Sur de Amazon Web Services. Mediante Memorando Nro. AN-APAM-2024-0021-M, de 15 de febrero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por la magíster Alexandra Manuela Arce Plúas, asambleísta. Mediante Oficio Nro. MDI-DMI-2024-0474-OF, de 18 de febrero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por la doctora Mónica Rosa Irene Palencia Núñez, ministra del Interior (E). Mediante Oficio Nro. FGE-DSP-2024-001378-O, de 19 de febrero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por la señora Diana Salazar Méndez, fiscal general del Ecuador. Mediante Oficio Nro. DGAC-DGAC-2024-0302-O, de 02 de febrero de 2024, la Comisión Especializada Permanente de Soberanía, Integración

y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por el ingeniero Oswaldo Roberto Ramos Ferrusola, director general de la Aviación Civil, encargado. Mediante correo electrónico oficial Zimbra de la Asamblea Nacional, de 26 de febrero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por la doctora Mónica Rosa Irene Palencia Núñez, ministra del Interior (E). La presidenta de la Comisión Especializada Permanente de Soberania, Integración y Seguridad Integral, invitó a los delegados de varias instituciones públicas a participar en varias mesas técnicas para revisión de los nudos críticos con respecto al texto borrador del Proyecto de Ley Orgánica de Seguridad Digital: Mediante Oficio Nro. AN-CSIS-2024-0043-SR, de 26 de febrero de 2024, al señor Diego Urbina, gerente de Región Sur de Amazon Web Services. Mediante Oficio Nro. AN-CSIS-2024-0044-SR, de 26 de febrero de 2024, al señor Polo Fabian Íñiguez, asesor de Grupo Radical. Mediante Oficio Nro. AN-CSIS-2024-0045-SR, de 26 de febrero de 2024, al señor magíster Javier Andrés Borja, experto en seguridad digital. Mediante Oficio Nro. AN-CSIS-2024-0107-O, de 27 de febrero de 2024, a la señora doctora Mónica Rosa Irene Palencia Núñez, ministra encargada del Ministerio del Interior. Mediante Oficio Nro. AN-CSIS-2024-0108-O, de 27 de febrero de 2024, al señor Gian Carlo Loffredo Rendón, ministro de Defensa Nacional. Mediante Oficio Nro. AN-CSIS-2024-0110-O, de 27 de febrero de 2024, a la señorita magíster Mishel Andrea Mancheno Dávila, secretaria general de la Presidencia de la República del Ecuador. Mediante Oficio Nro. AN-CSIS-2024-0113-O, de 29 de febrero de 2024, al señor doctor Álvaro Francisco Román Márquez, presidente del Consejo Nacional de la

Judicatura. Mediante Oficio Nro. AN-CSIS-2024-0114-O, de 29 de febrero de 2024, al señor Michele Sensi Contugi Ycaza, director del Centro de Inteligencia Estratégica (CIES). Mediante Oficio Nro. MDN-MDN-2024-0527-OF, de 29 de febrero de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital del señor Gian Carlo Loffredo Rendón, ministro de Defensa. La presidenta 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 revisión de los nudos críticos con respecto al texto borrador del Proyecto de Ley Orgánica de Seguridad Digital: Mediante Oficio Nro. AN-CSIS-2024-0118-O, del 04 de marzo de 2024, a la señora doctora Mónica Rosa Irene Palencia Núñez, ministra encargada del Ministerio del Interior. Mediante Oficio Nro. AN-CSIS-2024-0126-O, del 04 de marzo de 2024, al señor doctor Álvaro Francisco Román Márquez, presidente del Consejo Nacional de la Judicatura. Mediante Oficio Nro. AN-CSIS-2024-0127-O, del 04 de marzo 2024, al señor Michele Sensi Contugi Ycaza, director del Centro de Inteligencia Estratégica (CIES). Mediante Oficio Nro. AN-CSIS-2024-0128-O, del 04 de marzo de 2024, al señor Gian Carlo Loffredo Rendón, ministro de Defensa Nacional. Mediante Oficio Nro. AN-CSIS-2024-129-O, del 04 de marzo de 2024, al señor César Antonio Martín Moreno, ministro de Telecomunicaciones. Mediante Oficio Nro. AN-CSIS-2024-0130-O, del 04 de marzo de 2024, a la señorita magíster Mishel Andrea Mancheno Dávila, secretaria general de la Presidencia de la República del Ecuador. Mediante Memorando Nro. MDI-DMI-2024-0167-MEMO, de 05 de marzo de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, invitó al señor Guido

Patricio Núñez Torres, subsecretario de Seguridad Pública; a la señora magíster Sofía Estefanía Vázquez Izurieta, directora de Articulación Interinstitucional para la Seguridad Ciudadana; y a la señorita magíster María Daniela Álvarez Galarza, directora de Ciberdelitos encargada, a participar en varias mesas técnicas para la revisión de los nudos críticos, respecto al texto borrador del Proyecto de Ley Orgánica de Seguridad Digital. Mediante correo electrónico oficial Zimbra de la Asamblea Nacional, de 08 de marzo 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por la doctora Mónica Rosa Irene Palencia Núñez, ministra del Interior (E). Mediante Memorando Nro. AN-ABIM-2024-0051-M, de 12 de marzo de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por la señora Inés Margarita Alarcón Bueno, asambleísta. Mediante correo electrónico oficial Zimbra de la Asamblea Nacional, de 15 de marzo de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por el doctor Javier Andrés Borja, experto en seguridad digital. Mediante Oficio Nro. AN-CSIS-2024-0154-O, de 19 de marzo de 2024, la presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, solicitó aportes y observaciones al Proyecto de Ley Orgánica de Seguridad Digital a la señorita magíster Mishel Andrea Mancheno Dávila, secretaria general de la Presidencia de la República. Mediante Memorando Nro. AN-ABIM-2024-0059-M, de 21 de marzo de 2024, la Comisión Especializada Permanente de Soberanía, Integración y

Seguridad Integral, recibe las observaciones respecto al Proyecto de Ley Orgánica de Seguridad Digital, realizadas por la señora Inés Margarita Alarcón Bueno, asambleísta. La presidenta 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 revisión de los nudos críticos con respecto al texto borrador del Proyecto de Ley Orgánica de Seguridad Digital: Mediante Oficio Nro. AN-CSIS-2024-0155-O, del 19 de marzo de 2024, a la doctora Lady Diana Salazar Méndez, fiscal general del Estado. Mediante Oficio Nro. AN-CSIS-2024-0156-O, del 19 de marzo de 2024, al señor doctor Álvaro Francisco Román Márquez, presidente del Consejo Nacional de la Judicatura. Mediante Oficio Nro. AN-CSIS-2024-0157-O, del 19 de marzo de 2024, a la señora doctora Mónica Rosa Irene Palencia Núñez, ministra del Ministerio del Interior (E). En Sesión Nro. 032, realizada el 17 de abril de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral puso en conocimiento, debate y aprobación el texto borrador del Proyecto de Ley Orgánica de Seguridad Digital. En Sesión Nro. 037, realizada el 01 de mayo de 2024, la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral puso en conocimiento, debate y aprobación el informe del Proyecto de Ley Orgánica de Seguridad Digital. 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. Durante todo el proceso de socialización y tratamiento del Proyecto de Ley Orgánica de Seguridad Digital, se recibieron a representantes de la Función Ejecutiva, delegadas y delegados de instituciones públicas y representantes de organizaciones de la sociedad civil, las mismas que

se sintetizan a continuación: 2.2.1. Observaciones presentadas previo al informe para primer debate. 2.2.1.1. Observaciones instituciones y ciudadanas recibidas en comisión general. La Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, dio inicio al proceso de socialización del presente proyecto de ley a partir del 27 de agosto de 2021. La comisión, en 17 sesiones, recibió en comisión general a un total de 22 representantes institucionales de organizaciones de la sociedad civil, de la academia y expertas y expertos nacionales e internacionales. Las principales observaciones realizadas durante el tratamiento del informe para primer debate giraron en torno a los siguientes aspectos: 1. Necesidad de una ley orgánica que regule la seguridad digital, que busca fortalecer los procesos para la mitigación de los ataques digitales ya en curso y previamente identificados, disminuyendo o atenuando sus efectos maliciosos con el fin de alertar a otros usuarios para su preparación. 2. La ley reconoce principios fundamentales para la seguridad digital como la autenticidad (de la identidad digital), cooperación, integridad (de la información), disponibilidad (de contenido digital), integridad (de datos), oportunidad de acciones, de prevención y reserva de información. 3. La ley promueve la resiliencia y la recuperación ante incidentes digitales que, si bien pueden tener afectaciones considerables, también son una oportunidad de aprendizaje, de implementación de medidas de protección y de desarrollo de una cultura de seguridad digital a todo nivel. 4. Es importante desarrollar mecanismos de control, de modo que se asegure el cumplimiento de esta ley. En la siguiente tabla se resume 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 Nro. 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 dado 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 la 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 cómo 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, ¿qué hacer en estos casos?
Daniel Tenorio,	• Señala respecto del ente rector de seguridad digital que

experto en ciberseguridad	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 generaria mayor transparencia, pero de todas formas depende como sea abordada la ciberseguridad en los textos legales. • Finalmente, menciona que debemos suscribir los convenios internacionales que establecen estándares de ciberseguridad. Debemos dejar de ser victimas y empezar a aprender cómo defendernos.
Sesión Nro. 38 Fecha: 17/12/2021 Link: https://www.facebook.com/ComisionSoberaniaAN/videos/270071441846529/	
Sesión Nro. 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 ataques cibernéticos. • El proyecto de ley contiene 16 articulos, 4 reformatorias, 3 transitorias y una disposición final, que dan un total de 24 articulos. La materia trata de la seguridad digital desde la perspectiva de los subsistemas de ciberseguridad, ciberdefensa y ciberinteligencia, 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 soberania 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 los 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 brindará 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 Junta 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 Llumiquinga. • 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 la moción por escrito.

Acta 922-A

Sesión Nro. 64
Fecha: 03/12/2021
Link:
https://www.facebook.com/watch/live/?ref=watch_permalink&v=323632899320331
/

Alejandro Padín Vidal, experto en ciberseguridad	• 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 del Estado. • Los ataques más números son: malware, ataques en la web, phishing, etcétera. • 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. • 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, etcétera. • 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 ciberinteligencia. 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 más 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, ¿cómo funciona? ¿Igualmente, cómo 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 qué resultados han obtenido.
Rodrigo Fajardo, integrante de la comisión	• Solicita se aclare cómo se desarrolla 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 Nro. 98 Fecha: 08/03/2022 Link: https://www.facebook.com/ComisionSoberaniaAN/videos/460527749103271/	
José Luis Vallejo, integrante de la comisión	• 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. • Se ha evidenciado la desarticulación de los organismos competentes, falta de recursos, falta de legislación, etcétera. El Ecuador está en el puesto 118 de 189 países en materia de ciberseguridad. • Este proyecto tiene 3 bloques: 1) Ciberseguridad: el análisis se basa en la legislación española y EE.UU. 2) Seguridad sistémica: desarrolla una propuesta de funcionamiento del sistema de ciberseguridad, banco de alertas, etcétera. 3) Eje conceptual: contiene todo lo relativo a la tan anhelada seguridad integral.
Sesión Nro. 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 hiperconexión, es un mundo en donde la interacción en el ciberespacio crea un entorno de hiperregistro. Es un mundo donde existen pandemias de desinformación, es un ciberespacio 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 ciberespacio 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 Secretaría del Consejo de Ciberseguridad, etcétera. • 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, etcétera. • En el caso de existencia de amenazas o ataques, la ley se aplica cuando el ataque se dé en redes o cuando la ciberamenaza o infraestructura determinada por el consejo de Ciberseguridad, o cuando se afecte a infraestructura crítica o estratégica. • Una vez se revisa la primera parte del proyecto, el sistema de ciberseguridad incluye a 12 actores, entre los cuales están el ente rector de la política de defensa, de telecomunicaciones, Conartel, Fiscalía, Superintendencias, INEC, etcétera. 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 Ciberseguridad y la Agencia de Ciberseguridad, 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 Nro. 132 Fecha: 15/06/2022 Link: https://www.facebook.com/ComisionSoberaniaAN/videos/383684143592752/	
Coronel Victor Nieto, delegado del 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 criticos 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, deberian 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 Cancilleria	• Responde asegurando que la Cancilleria 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 del 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 ciberseguridad. Es importante señalar que el Comité Nacional de Ciberseguridad ha venido sesionado de manera permanente para desarrollar una política contra la ciberdelincuencia y ciberseguridad. Estos términos son muy amplios y más bien sugerimos que se cambie este término por ciberdelito. • El ciberdelito se encarga de investigar los delitos tecnológicos, mientras que la ciberseguridad previene los incidentes informáticos. Se han realizado observaciones técnicas a este documento y venimos trabajando con Policía Nacional.
Fabián Íñiguez, subsecretario del Ministerio de Telecomunicaciones	• Señala que se ha buscado sentar las bases de una nueva política de ciberseguridad, a través de la constitución del Comité Nacional de Ciberseguridad, compuesto por el Ministerio de 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 privado 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 ciberdelitos. Trabajamos con las superintendencias, quienes nos han dado aportes para este tema. Además, con infraestructura crítica del Estado, los GAD, etcétera. • 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 Narvácz, presidente de la comisión	• Pregunta: ¿qué estructura es la más adecuada para generar política pública en materia de seguridad digital?, ¿hay un diagnóstico en ciberseguridad en nuestras instituciones?, ¿por qué se junta ciberseguridad y ciberinteligencia, es pertinente, acaso no tiene su propia naturaleza?
Fabián Íñiguez, subsecretario del Ministerio de Telecomunicaciones	• Destaca que la Ley Orgánica de Telecomunicaciones, en el artículo 140, determina que el ente rector en seguridad de la información es el Mintel. La Seguridad de la información abarca ciberseguridad, ciberdefensa y ciberinteligencia, 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 ciberseguridad, ciberdefensa, ciberinteligencia, pero falta la ciberdiplomacia y ciberdelitos. 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 del Ministerio de Telecomunicaciones	• Se ha aportado en el Comité de Ciberseguridad, 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 habla de ciberdefensa, que ya está regulada en la normativa del Ministerio de Defensa, la ciberseguridad está definida por el Ministerio del Interior, pero la ciberinteligencia es una transversalidad. • La UAFE aporta en función de los casos que se analizan.
Vianna Di María Maino Isaías, ministra de Telecomunicaciones	• 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 esté actualizada para dar certeza

y Sociedad de la Información	en las transacciones financieras, cibernegocios, etcétera. • Es importante que estos conceptos acojan las mejores prácticas internacionales porque el ciberespacio 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 adecúe a la Convención de Budapest. • La otra mención hace referencia a la estrategia nacional de ciberseguridad que ha sido construida con prácticas internacionales, el lanzamiento será el día jueves, con ayuda del Gobierno de Estonia. • Exhorta a los señores asambleistas que ellos como ente regulador deben asegurar una continuidad y las estrategias que debe verse reflejada en la norma.
Sesión Nro. 133 Fecha: 15/06/2022 Link: 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.

- 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 considerar: 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, etcétera. 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 datos 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, etcétera. 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 públicos y privados, y si el conjunto de controles tecnológicos de ciberseguridad se basa en marcos de ciberseguridad 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, aun cuando esté 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 Enriquez 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 periodo determinado y magnitud (impacto primario y secundario). • Las definiciones de confidencialidad, integridad y disponibilidad deberían 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 ciberamenaza) por sí 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 27005 ISO y las cinco etapas de la gestión de riesgos (seguridad proactiva). • Menciona que en el artículo 6.5 hay pérdida de autenticidad, revisar conformidad con la Ley Orgánica de Protección de Datos. Las medidas de control harían que se pierda un sistema de autenticidad si no 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 artículo 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 qué fraude en función de la ley. Ejemplo: no es lo mismo fraude informático que falsificación informática. Referencia (Convenio de Budapest delincuencia informática con fin, delincuencia informática como medio, delitos de contenido). • No existe definición de delitos digitales, reemplazar o 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 semicuantitativo. • 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 multidimensionalidad 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 Nro. 157 Fecha: 24/08/2022 Link: https://www.facebook.com/ComisionSoberaniaAN/videos/478108654138566/	
Diego Urbina, asesor en materia de política pública de 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 desarrolló tecnología para sus propios servicios, pero que luego se vendió al público. En 2006 surge el concepto de información en la nube. • ¿Qué 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, etcétera. 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 a 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 deberian ser unificados en uno solo, se debe modificar el articulo 146 de Código Ingenios que regula la ubicación de los servidores de las entidades pùblicas. 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 especifico, 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 asi. Uno pensaria 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 Nro. 160 Fecha: 31/08/2022 Link: https://www.facebook.com/watch/live/?ref=watch_permalink&v=1191674628065676	
Humberto Arthos, delegado de la Agencia de Regulación y Control	• 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

de las Telecomunicaciones (Arcotel)	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 cómo se procesan y analizan los datos, y la ciberdefensa guarda relación con la protección de la soberania. • 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, etcétera. 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 deberia homologar los articulos que tienen definiciones, para evitar la contraposición con leyes vigentes (datos, telecomunicaciones, normativa internacional, etcétera). 2. La estructura del sector y de la nueva entidad debe ser trabajada entre todas las partes involucradas. 3. Definir qué 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: ciberinteligencia, ciberdefensa 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, etcétera. 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 Nro. 162 Fecha: 07/09/2022 Link: https://www.facebook.com/ComisionSoberaniaAN/videos/744584409937308/	
Jonathan Ramos, docente de derecho penal UCE y representante de la Asociación Académica Ecuatoriana de Derecho e Información	• 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 ciberdelincuencia, 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 ciberespionaje 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 determina la responsabilidad en un hecho delictual. Respecto de la interceptación de datos, señala

	que la asistencia de un proveedor internacional sin autorización formal, se podria 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 Nro. 164 Fecha: 09/09/2022 Link: https://www.facebook.com/ComisionSoberaniaAN/videos/462078729165709/	
Marcelo Gómez, delegado del Centro de Inteligencia Estratégica	• Señala que los dominios de intervención del Estado son mar, aire y espacio, pero ahora se incorpora como otro dominio el ciberespacio. La SNAI y 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 críticas 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 estar 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. Y 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 crítica, 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 qué 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 Cancilleria con ciertas novedades en el servicio.
Sesión Nro. 209 Fecha: 23/02/2023 Link: 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 que 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 ciberseguridad, 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 primer debate, mismo que cuenta con 79 artículos, que abordan la estructura del 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 grandes 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 artículo 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, etcétera, 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 artículo 3 numeral 9, dice promover la confianza para el intercambio de información y la gestión de conocimiento de seguridad en el ciberespacio. 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 del Interior y que tiene como objetivo evitar la vulneración de derechos, a través de los procesos que lleva adelante 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 Nro. 211 Fecha: 24/02/2023 Link: https://fb.watch/jgqYLXqRaz/	
Melania Carrión,	• Menciona que el cumplimiento de las funciones se da a

asesora de la comisión	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 asambleista 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	• Señala que no sería necesario en razón de que esta ley no establece nada en materia jurisdiccional.

comisión	
Patricia Núñez, vicepresidenta de la comisión	• ¿Cómo 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 estadistica, etcétera. 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 seria 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 especifica, 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 Soberania, Integración y Seguridad Integral.

2.2.1.2. 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. ----------

Nro.	Institución. Organismo. Organización. Ciudadano.	Aspectos observados.
	Coronel (SP) Fausto Cobo, director general del Centro de Inteligencia Estratégica. Oficio Nro. CIES-CIES-0108-2022-OF.	• Observaciones Ley de Seguridad Digital: - 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". - 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: - 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,

Nro.	Institución. Organismo. Organización. Ciudadano.	Aspectos observados.
		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 politica pública. • Sugiere incluir la siguiente definición. Ciberamenaza: Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de este. 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, 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

Nro.	Institución. Organismo. Organización. Ciudadano.	Aspectos observados.
		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 criticas (...). 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 podrian 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 Secretaria 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 Secretaria 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 critica 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 apoyar y resolver cualquier incidente que tenga lugar dentro del pais 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 podrian provocar incidentes a los componentes de tecnologia 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

Nro.	Institución. Organismo. Organización. Ciudadano.	Aspectos observados.
		responsabilidad en el uso de la tecnología, de manera especifica 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 soberania del Estado y la protección de la infraestructura critica y servicios esenciales. En relación a las funciones del subsistema, será ciberdefensa además de 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 podria 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

Nro.	Institución. Organismo. Organización. Ciudadano.	Aspectos observados.
		riesgos. 3. Coordinar 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 entorno 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. - 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 la 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 artículo 11. - Propone una nueva definición de ciberinteligencia: actividades de inteligencia en soporte de la ciberseguridad. Se trazan ciberamenazas, se analizan las intenciones y oportunidades de los

Nro.	Institución. Organismo. Organización. Ciudadano.	Aspectos observados.
		ciberadversarios 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 una 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 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 ha funcionado de manera excelente en otros países.
	Coronel (SP) Fausto Cobo, director general del Centro de Inteligencia Estratégica. Oficio Nro. CIES-CIES-0195-2022-OF	• Presenta una propuesta de unificación de los tres proyectos de ley.
	General (SP) Luis Lara Jaramillo, ministro de Defensa	• Observaciones Proyecto Ley de Seguridad Digital: - 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.

Nro.	Institución. Organismo. Organización. Ciudadano.	Aspectos observados.
	Nacional. Oficio Nro. MDN-MDN-2022-0982-OF.	- 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 FF.AA., 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 servicios digitales, considerando su organización, estructuración, conservación, adaptación, modificación, extracción, consulta, utilización, etcétera. - 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

Nro.	Institución. Organismo. Organización. Ciudadano.	Aspectos observados.
		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, etcétera. - Sugiere cambiar el nombre sistema nacional de ciberseguridad por sistema nacional de seguridad digital, con la finalidad de mantener armonia 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.

Nro.	Institución. Organismo. Organización. Ciudadano.	Aspectos observados.
		- 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 politica pública de defensa, sugiere eliminar el literal relativo a la respuesta a las ciberamenazas 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 politica 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 politica pública de seguridad ciudadana y convivencia social pacifica, sugiere incluir: Fortalecer la capacidad estratégica de ciberseguridad del Estado; y, de igual forma, eliminar el numeral relativo a la respuesta a las ciberamenazas 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 politica pública de telecomunicaciones, sugiere eliminar el literal relativo a la respuesta a las ciberamenazas y ciberataques mediante acciones tácticas, oportunidad y estratégicas, recopilar pruebas o evidencias; y, reporte de los resultados a la Agencia Nacional de

Nro.	Institución. Organismo. Organización. Ciudadano.	Aspectos observados.
		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.

2.2.1.3. Detalle de la socialización realizada por la comisión. La Comisión de Soberanía, Integración y Seguridad Integral, durante un total de 10 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
Nro. 20 06 de agosto de 2021	• Conocer el Proyecto de Ley de Seguridad Digital presentado por el exasambleísta Juan Carlos Yar.
Nro. 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.
Nro. 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.

REPÚBLICA DEL ECUADOR

Asamblea Nacional

Acta 922-A

Sesión fecha	Puntos tratados
Nro. 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.
Nro. 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.
Nro. 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.
Nro. 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.
Nro. 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.
Nro. 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.
Nro. 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. 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.

REPÚBLICA DEL ECUADOR

Asamblea Nacional

Acta 922-A

Sesión fecha	Puntos tratados
Nro. 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.
Nro. 160 31 de agosto de 2022	• Con la finalidad de recibir sus observaciones y recomendaciones, los proyectos de ley sobre ciberseguridad presentados por el exasambleísta 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).
Nro. 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 exlegislador 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: • Magister Jonathan Marcelo Ramos Mera, catedrático de derecho penal de la Universidad Central del Ecuador y representante de la Asociación Académica Ecuatoriana de Derecho e Informática.
Nro. 164 9 de septiembre de 2022	• 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 exlegislador 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.
Nro. 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.

2.2.1.4. 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	ago-21		sep-21	nov-21	dic-21	mar-22		abr-22	jun-22		
Asambleísta / Fecha	6	27	17	24	3	8	30	6	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 Nùñez	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	
Asambleista/ 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	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 Gallas	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 Nûñez	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:

Nota*: La asambleista Gissela Castillo es alterna del asambleista Rodrigo Fajardo y fue posesionada mediante Memorando Nro. AN-FCRO-2022-0071-M. Nota**: La asambleista Eleana Romero es alterna del asambleista 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 asambleista Geraldine Weber y fue posesionado mediante Memorando Nro. AN-WMG-2022-0054-M, mismo que modificó al Memorando Nro. AN-WMG-2022-0053-M.

2.2.2. Observaciones presentadas durante el tratamiento previo al informe para segundo debate. Durante el tratamiento del proyecto de ley previo al informe para el segundo debate, se presentaron un total de 45 observaciones, las mismas que fueron procedas y analizadas por la comisión. En los siguientes apartados se sintetiza las principales observaciones presentadas por las señoras y señores asambleístas durante el primer debate, las observaciones remitidas por escrito, las observaciones institucionales y de actores de la ciudadanía. 2.2.2.1. Observaciones presentadas en el Pleno de la Asamblea Nacional. Durante el primer debate del Proyecto de Ley Orgánica de Seguridad Digital, en la Sesión Nro. 862 del Pleno de la Asamblea Nacional, convocada para el día 20 de abril del 2023, intervinieron un total de ocho legisladoras y legisladores, cuyos comentarios, observaciones y una síntesis del procesamiento de las observaciones, se presentan a continuación: Tabla 6. Observaciones presentadas durante el primer debate. ----------

Ley Orgánica de Seguridad Digital	
Sesión Nro. 862 Fecha: 20/04/2023 Link: https://www.youtube.com/live/AygWfYGg2p4?si=CmKGsQ8osgYjas8d/	
José Luis Vallejo, asambleista por Carchi	• Sugiere incluir la definición de trazabilidad. • Señala que se deben regular los derechos digitales en el ciberespacio, recomienda que en el artículo 6 se incorpore "x". • El Centro de Respuesta Incidentes Informáticos debe ser la base de este centro. • En las sociedades digitales, los datos son el nuevo metal precioso. Esta normativa es un deber de los Estados. • Si la inseguridad ha sido un legado del Ejecutivo, hagamos que la ciberseguridad sea el legado del Legislativo.
Geraldine Weber, asambleista por Guayas	• Hoy estamos más conectados que nunca. • Se han dado varios ataques, incluso a la Contraloría. El riesgo de ciberataques necesita de medidas reguladas y normas legislativas, para proteger los sistemas de información. • La pérdida de seguridad, la vulnerabilidad depende de esta ley. • Es fundamental proteger a los ciudadanos.

	• El presente informe pone en conocimiento estas iniciativas del asambleista Rodrigo Fajardo, José Luis Vallejo y el exlegislador Juan Carlos Yar. • Esta ley establece un sistema nacional de seguridad digital y sus subsistemas. • Esta ley establece una serie de derechos para que los usuarios puedan gozar el derecho a la privacidad. • Además, busca promover la confianza digital. • Se debe fomentar la alfabetización digital para impulsar una sociedad segura en el uso de la tecnología digital. • El proyecto busca convertirnos en un referente regional y mundial en la materia. • Promueve la ley de propiedad intelectual, protección de datos, etcétera. • Los proveedores de los servicios de internet deben prestar su servicio en todo el país, sin discriminación. • Se busca garantizar un entorno digital para todos.
Luis Almeida, asambleísta por Guayas	• Realiza un discurso político.
Simón Bolívar Remache, asambleísta por Santa Elena	• El país necesita de este proyecto de ley, ya que la tecnología ha creciendo y desarrollado de una manera acelerada que el país requiere estar a esa altura.
Celestino Chumpi, asambleísta por Morona Santiago	• Hace referencia a la nacionalidad Shuar de la Amazonía, indicando que se pretende decir algo de las lanzas que solo pueden usar los indígenas. • Deberíamos tener el control de las redes sociales, somos famosos para atacar aún sin fuentes de información real. • Debemos tener el control de los trolls centers.
Juan Fernando Flores, asambleísta por América Latina, El Caribe y África	• Este es un proyecto de ley importante, hemos visto cómo avanza en el mundo los avances tecnológicos, el acceso a la información, etcétera. • Cómo se garantiza que de manera certera exista seguridad para cada ciudadano. • Se debe determinar si esta ley es solo para el sector público, sino para todos los sectores. • Ya hemos tenido eventos de inseguridad en el sector privado. • Realiza observaciones a las definiciones realizadas en el proyecto: En el caso del artículo 27 que abarca a varias instituciones. Se debe reconsiderar cuáles son los sujetos que se han incorporado en el sistema y si son ellos los adecuados para responder. • En el artículo 33 se debe precisar cómo va a participar el Consejo de la Judicatura en este proceso. • Cómo vamos a garantizar estas acciones en el presupuesto, trabajando bien y de forma delimitada. Cómo garantizamos la aplicación de esta norma. • Muchos ciudadanos tienen temor de usar las plataformas, debemos garantizar que la aplicación de la norma en el sector público y privado sea eficaz.

	• Estamos viviendo momentos globalizados en los que la tecnología avanza a cada instante. • Cuando ha existido fuga de información desde sector privado o público, existan garantías, ya que los ecuatorianos exigen seguridad.
Stalin Bayas, asambleísta por Azuay	• Es un proyecto de ley muy importante. El país necesita leyes que vayan en beneficio de la sociedad y esta ley es una de ellas. • Debe existir el compromiso de los jueces y fiscales para erradicar la delincuencia.
Nataly Viteri, asambleísta por Chimborazo	• Sugiere establecer acciones para la adhesión al Convenio de Budapest. • Se recomienda que la ley contenga un análisis de adecuación del Convenio de Budapest y sus protocolos con los derechos humanos reconocidos por el Ecuador. • Llevar a cabo mediante mesas de trabajo y consultas con los ciudadanos, organizaciones y academia con los principales instrumentos internacionales vigentes, aspectos en su implementación para evitar posibles y principales abusos gubernamentales en la implementación del Convenio de Budapest sobre ciberdelincuencia. Invitar a profesionales de otros países que ya han suscrito este convenio en América Latina para la cooperación jurídica internacional y retroalimentar el proceder respecto al proyecto de ley. • Se debe recibir el mayor número de aportes para esta ley y se hará llegar los aportes a la comisión para que sean analizadas.

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

2.2.2.2. Observaciones de las legisladoras y legisladores al informe del primer debate, remitidas por escrito para procesar al informe de segundo debate. Tabla 7. Observaciones de las legisladoras y legisladores presentadas por escrito. ----------

Remitente Fecha de documento	Síntesis de observaciones
Magíster Alexandra Arce, asambleísta por Guayas Memorando Nro. AN-APAM-2024-0021-M, del 15 de febrero de 2024	Presenta observaciones a dos artículos del proyecto de ley, entre las que se puede resaltar las siguientes: • Primero: De lo analizado, he notado que el artículo 18 inciso segundo del presente anteproyecto es una norma que carece de claridad y provoca inseguridad jurídica. Habla de investigación sin especificar a qué tipo se refiere, es decir, que se podría hacer dentro de una investigación de índole laboral, tributario, etcétera. Así mismo, al

Remitente Fecha de documento	Síntesis de observaciones
	referirse a causa judicial deja la puerta abierta para que se intercepte una comunicación, se recopilen datos en cualquier materia. Señalar: "o previa autorización de autoridad competente", rompe una de las exigencias establecidas en la Constitución que ha otorgado la exclusividad de autorización de este tipo de restricciones de los derechos constitucionales al juez y no a otra autoridad pública. El artículo en análisis no establece como requisito previo para la vigilancia, interceptación de las comunicaciones, tratamiento o recopilación de datos el plácet judicial, sino que permite estas intervenciones cuando se dé una de las siguientes circunstancias: una investigación, causa judicial o previa autorización de autoridad competente. En definitiva, resulta ser un artículo contrario a la Constitución que exige para la afectación de los derechos constitucionales la autorización judicial. A más de lo anterior, no se ha tomado en cuenta lo estipulado en el artículo 476 del COIP, que ha incorporado para la aplicación de esta clase de restricciones los principios de idoneidad, necesidad y proporcionalidad. • Segundo: Sobre el artículo 57, tenemos duda en torno a si vía esta ley se le puede exigir que la Fiscalía semestralmente presente reporte al ente rector del sistema y del Comité Nacional de Seguridad Digital. Esta interrogante surge porque la Constitución señala que esta entidad es un órgano autónomo de la Función Judicial, único e indivisible, funcionará de forma desconcentrada y tendrá autonomía administrativa, económica y financiera. • Tercero: El artículo 18 del proyecto de esta ley quiere arrogarse funciones que le competen a la Fiscalía o al departamento de inteligencia que, según las competencias de estas entendidas pueden, según el caso, intervenir las comunicaciones telefónicas. Por lo que debería en todo caso establecer como responsables de la investigación de casos de ciberataques a estas instituciones. • Esta ley, como sucede con la chilena, debería ir encaminada a establecer los estándares y establecer las directrices técnicas sobre seguridad de la información y ciberseguridad, que deberán cumplir los órganos de la administración del Estado para resguardar la confidencialidad, integridad, disponibilidad de la información y la infraestructura informática de las plataformas electrónicas. • Obligar a las instituciones gubernamentales y empresas privadas a que mejoren la gestión de su ciberseguridad. • En definitiva, lo principal de la ley de seguridad digital debe ser la de crear mecanismos que protejan los datos de la ciudadanía en el ciberespacio, sin embargo, de conformidad a lo argumentado supra, con el 18 se estaría vulnerado los

Acta 922-A

Remitente Fecha de documento	Síntesis de observaciones
	derechos constitucionales a la inviolabilidad de las comunicaciones, así como a la protección de datos.
Señora Inés Alarcón Bueno, asambleísta por Pichincha Memorando Nro. AN-ABIM-2024-0051-M, del 12 de marzo de 2024	Presenta observaciones a siete artículos del proyecto de ley, entre las que se puede resaltar las siguientes: • Sugiere incluir en el artículo 8. Activos de información de alto impacto. El Sistema Nacional de Seguridad Digital mitigará los riesgos y amenazas ante posibles vulnerabilidades a los activos de información (...). • Indica que se analice el incluir en el artículo 13. Enfoque de planificación estratégica. La seguridad digital se orientará por el Plan Nacional de Seguridad Integral, elaborado por el Cosepe (...). • Sugiere incluir en el artículo 42. Subsistema de Ciberdefensa. El subsistema de Ciberdefensa tendrá rectoría por parte del Estado, conformando un comité con las principales instituciones rectoras de seguridad para la toma de decisiones cuando existan riesgos, amenazas y/o posibles vulnerabilidades detectadas, ejecutadas con atacantes externos e internos que atenten contra la soberanía del Estado y/o se convierta en un delito tipificado en el COIP que cause conmoción interna, no gobernabilidad y democracia con la coordinación 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. • Indica la sugerencia en el artículo 44. Atribuciones del ente rector de la Defensa Nacional, numeral 5 se sugiere lo siguiente: 5) Fortalecer la capacidad estrategia y tecnológica de las instituciones públicas de seguridad que participan en ciberdefensa; y en el numeral 13 se sugiere lo siguiente: 13) Identificar los componentes de infraestructura informática que poseen un alto riesgo en relación con la defensa nacional en organismos públicos y privados conforme a la normativa nacional correspondiente. • Sugiere incluir en el artículo 47. Atribuciones del ente rector de seguridad ciudadana, protección interna y orden público en materia de ciberseguridad ciudadana. 5. Fortalecer la capacidad estratégica y tecnológica de las instituciones públicas de seguridad que ejecutan acciones en materia de ciberdefensa. • Sugiere incluir la siguiente definición: Inteligencia artificial: Sistema de inteligencia artificial que se desarrolla empleando una o varias técnicas y estrategias que figuran en un conjunto determinado de objetivos definidos por seres humanos, generando información de salida como contenidos, predicciones, recomendaciones y/o decisiones que influyan en los entornos con los que interactúa.

Remitente Fecha de documento	Síntesis de observaciones
	• Se sugiere incluir un artículo sobre la inteligencia artificial: Mintel deberá generar políticas de uso y aplicación de inteligencia artificial dentro del ciberespacio en territorio ecuatoriano, determinando hasta qué punto se considera una aplicación administrativa con la creación de normativa. Arcotel supervisará el desarrollo sostenible de aplicación sobre sistemas algorítmicos de inteligencia artificial, su aplicación en el marco normativo y la minimización de los riesgos que puede suponer el uso de esta nueva tecnología. Dará a conocer oportunamente a la institución de seguridad pertinente en caso de generarse una acción que se enmarque dentro de una acción tipificada por la ley.
Señora Inés Alarcón Bueno, asambleísta por Pichincha Memorando Nro. AN-ABIM-2024-0059-M, de 21 de marzo de 2024	Presenta observaciones a tres artículos del proyecto de ley, entre las que se puede resaltar las siguientes: Dentro del marco de construcción para el informe de segundo debate del proyecto de Ley Orgánica de Seguridad Digital, en concordancia con las disposiciones determinadas en la Ley Orgánica de la Función Legislativa, propongo las siguientes observaciones: 1. Dentro del capítulo II referente a principios y definiciones, realizo las siguientes observaciones: a) Observaciones: Incluir el término y definición de "confidencialidad" de la siguiente forma: "Confidencialidad. Consiste en el nivel de privacidad requerido para garantizar la protección de la información de los datos personales que será accesible o compartida solamente a los usuarios autorizados, ya sean estas personas naturales o jurídicas". b) Observaciones: Incluir la palabra: "y no estatales" dentro del concepto de "amenaza establecido" en el proyecto. Amenaza. Se considera amenaza a todo tipo de fenómenos, elementos o condiciones naturales o antrópicas dirigida a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste; caracterizadas por su capacidad, motivación e intencionalidad de atentar contra los intereses vitales o estratégicos del ciudadano o del Estado, en el ámbito de la seguridad digital. Estas amenazas pueden originarse desde diversas fuentes, como actores estatales y no estatales, ciberdelincuentes, ciberactivistas, ciberterroristas, competidores comerciales y otros. 2. Dentro de la sección tercera, la cual hace referencia al subsistema de ciberinteligencia, propongo lo siguiente: a) Se sugiere el siguiente texto alternativo al artículo 59 numeral 16, para que conste en la norma de la siguiente manera: "Artículo 59. Atribuciones del ente rector del sistema nacional de inteligencia. (...). 16. Definir las acciones y recursos estratégicos, operativos y tácticos

Remitente Fecha de documento	Síntesis de observaciones
	con las instituciones integrantes del sistema nacional de seguridad digital, a fin de contar con inteligencia, contrainteligencia estratégica y el desarrollo de prevención contra la desinformación digital". b) Se sugiere el siguiente texto alternativo al artículo 62 numeral 17, para que conste en la norma de la siguiente manera: Artículo 62. Atribuciones y funciones del ente rector en materia de relaciones exteriores y movilidad humana. 17. Las demás establecidas en la Ley, el reglamento general de aplicación y las determinadas por el Comité Nacional de Seguridad Digital. Observaciones: Se reemplazó "cibernética" por "digital".

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

2.2.2.3. Observaciones institucionales y ciudadanas remitidas por escrito. El presente informe para segundo debate incorporó el procesamiento de las observaciones presentadas por instituciones, organizaciones de la sociedad y ciudadanía, de conformidad con el siguiente resumen: Tabla 8. Observaciones instituciones y ciudadanas remitidas por escrito previo al informe para segundo debate. ----------

Remitente Fecha documento	Síntesis de observaciones
Señora María Gabriela Sommerfeld Rosero, ministra de Relaciones Exteriores y Movilidad Humana Oficio Nro. MREMH-MREMH-2024-0030-OF, de 10 de enero de 2024	Presenta observaciones a ocho artículos del proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 4, en el principio de cooperación, cambiar la palabra respecto por respeto. Artículo 4. Principios. (...) "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 respeto 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". • Artículo 5. Definiciones, en ciberdiplomacia, cambiar la palabra del por de "ciberdiplomacia. Son las acciones realizadas por el ente rector de relaciones exteriores y movilidad humana (...)". • En el artículo 5. Definiciones, en datos relativos al tráfico, se reestructuró la definición de datos relativos al tráfico para un mejor entendimiento. "Datos relativos al

Remitente Fecha documento	Síntesis de observaciones
	tráfico. Son todos los datos relativos a una comunicación realizada por medio de un sistema informático. Estos datos son generados por el sistema como un componente integral de la cadena de comunicación y abarcan detalles cruciales, como el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación, así como el tipo de servicio subyacente". • En el artículo 11 se sugiere cambiar la palabra internaciones por internacional. • En el artículo 30, se propone que la rectoría del sistema nacional de seguridad digital la ejerza el Ministerio de Defensa y el CIES. • En el artículo 31, se propone que la rectoría del sistema nacional de seguridad digital la ejerza el Ministerio de Defensa y el CIES. Cambiar la palabra "a" por "de". • En el artículo 33, en los numerales 3 y 8, se repite el integrante del Comité Nacional de Seguridad Digital, por lo que se recomienda eliminar al integrante del numeral 2, al estar considerado en el numeral 8. • En el artículo 37, se sugiere cambiar la palabra "en" por "el". • En el artículo 53 numeral 5, se indica incluir la palabra, recopilar, procesar y analizar información con la finalidad de (...).
Señor Michele Sensi Contugi Ycaza, director general del Centro de Inteligencia Estratégica – CIES Oficio Nro. CIES-CIES-2024-0021-OF, de 29 de enero de 2024	Presenta observaciones a tres artículos del proyecto de ley, entre las que se pueden resaltar las siguientes: • El Centro de Inteligencia Estratégica, realiza la siguiente propuesta de articulado 1: "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 y la seguridad sistémica del Estado Ecuatoriano en el ciberespacio, proteger la seguridad de las infraestructura crítica y servicios esenciales; establece y regula el Sistema Nacional de Seguridad Digital y sus subsistemas de ciberseguridad, ciberdefensa, ciberinteligencia y ciberdiplomacia; promover la coordinación y articulación institucional e internacional, prevenir, gestionar, investigar y enfrentar amenazas en el ciberespacio; 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". • De las sugerencias realizadas al proyecto de norma en las mesas técnicas de trabajo, por parte del CIES, se observó en reiteradas ocasiones al capítulo II. Entidades de rectoría, coordinación y gestión incidentes digitales, artículo 30 del proyecto a la Ley Orgánica de Seguridad Digital, que prescribe lo siguiente: "Rectoría del Sistema Nacional de Seguridad Digital. La rectoría del sistema la

Remitente Fecha documento	Síntesis de observaciones
	tendrá el ministerio rector de las telecomunicaciones y de la sociedad de la información"; al respecto, es menester indicar que el Ministerio de Telecomunicaciones y de la Sociedad de la Información, es un ente normativo en temas de seguridad de la información, lo recomendable y expuesto en las sesiones de trabajo, previas a la elaboración del informe para primer debate, se argumentó ampliamente y sugirió sea uno diferente, el contexto de la futura ley haría que se convierta en juez y parte en el ámbito de la seguridad digital. • Con respecto a los ítems antes referidos, el subrayado del primer ítem es lo que se sugiere sea incluido en el artículo 1, fue tema de amplio argumento en las convocatorias a las sesiones de trabajo con diferentes actores en las sesiones de construcción del informe para primer debate; en cuanto al segundo ítem, se ha considerado lo expuesto en el mismo a efecto de que se revise la consecuencia de que un mismo organismo sea el encargado de la normativa y del control de cumplimiento de la futura ley. • Es menester indicar que, de las mesas de trabajo en las que ha participado el Centro de Inteligencia Estratégica, ante la Comisión de Soberanía, Integración y Seguridad Integral de la Asamblea Nacional, se ha observado, en el artículo 55 numeral 7, en su parte pertinente al uso del término crítica digital, mencionado que, a lo largo del proyecto de normativa, no se utiliza el término y solo se emplea para "infraestructura crítica".
Doctora Ana María Larrea Maldonado, directora ejecutiva del Consorcio de Gobiernos Autónomos Provinciales del Ecuador (Congope) DE-2024-047-O, de 29 de 2024	Presenta observaciones a tres artículos del proyecto de ley, entre las que se pueden resaltar las siguientes: • Si la ley es orgánica y en el objeto de esta hablamos de derechos humanos, creo que es importante describir en la ley los derechos en el entorno digital, es así como se debería incluir un artículo de la siguiente manera: Derechos en el entorno digital. Todas las personas poseen idénticos derechos en el entorno digital y en el analógico, sin perjuicio de las limitaciones que, de acuerdo con la normativa, pudieran establecerse atendiendo a las peculiaridades de cada ámbito. Sin embargo, se promoverá la igualdad en el ámbito digital, de conformidad con el desarrollo y el uso de la tecnología, así como cualquier proceso relacionado con ellos deberán tener presente la exigencia de garantizar la dignidad humana, los derechos fundamentales, el libre desarrollo de la personalidad y procurar el logro del bien común. • En el último inciso del artículo 2 sobre el ámbito se establece una generalidad para toda la norma respecto del cumplimiento de la Ley Orgánica de Protección de Datos Personales, por ese motivo creo la necesidad de

Remitente Fecha documento	Síntesis de observaciones
	este inciso eliminarlo del artículo e incluirlo en una disposición general de la siguiente manera: disposición general tercera. Las disposiciones de la presente ley son aplicables sin perjuicio del cumplimiento de las disposiciones de la Ley Orgánica de Protección de Datos Personales. • En el artículo 31, considero que para cumplir con el objetivo de la ley, dentro de las atribuciones del ente rector del sistema nacional de seguridad digital, se debe incluir la creación de un equipo especializado, a manera de consejo consultivo, en seguridad digital, equipo que podrá ser formado por servidores públicos o trabajadores del sector privado, que podría ser llamado, a consideración del ente rector del sistema, en caso de un amenaza, riesgo, incidente, ataque o crisis cibernética en cualquiera de las instituciones miembros del sistema para una inmediata respuesta al problema causado, numeral que iría de la siguiente manera: 27. Crear un equipo especializado, a manera de consejo consultivo, en seguridad digital, equipo que podrá ser formado por servidores públicos o trabajadores del sector privado, para dar inmediata respuesta en caso de amenaza, riesgo, incidente, ataque o crisis cibernética en cualquiera de las instituciones miembros del sistema. Este consejo podrá ser llamado a consideración del ente rector del sistema.
Doctor Holguer Jaime Canseco Guerrero, director general del Consejo de la Judicatura Oficio-CJ-DG-2024-0022-OF, de 10 de enero de 2024	El Consejo de la Judicatura remite la matriz de análisis del Proyecto de Ley Orgánica de Seguridad Digital, presentando observaciones a 13 artículos y la creación de 4 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • Se conforma por: 10. La máxima autoridad del Consejo de la Judicatura o su delegado permanente. El reglamento a la presente ley establecerá la organización y funcionamiento del comité. Reuniones trimestrales. Artículo 34. Atribuciones del CNSD. • Artículo 40. Funciones del Centro Nacional de Respuesta a Incidentes de Seguridad Digital. Incluir 2. Coordinar y articular acciones con los centros de respuesta a incidentes de las entidades públicas y privadas (...). • En el artículo 3, se va a crear estas unidades y a qué estructura del Estado va a pertenecer. • En el artículo 4, en la definición autenticidad, no hace referencia a qué tráfico se refiere. • En el artículo 4, en la definición de cooperación, existe error de redacción, ajustar la palabra respecto por respeto. • En el artículo 5, agregar a continuación de sistemas públicos o privados. Esto para mayor comprensión. • En el artículo 18, es decir, deberán estar implementadas

Remitente Fecha documento	Síntesis de observaciones
	la Lotda, LOPP. • Crear un artículo, posterior al artículo 24 debe existir un artículo que defina y clasifique los incidentes digitales en bajos, medios y alto impacto y los tiempos en los que debe atenderse. • En el artículo 25, agregar plan de contingencia para informar a la ciudadanía. • En el artículo 26, está articulado por instituciones. Así mismo, se deberá crear un ente estatal con autonomía financiera para el cumplimiento de las actividades de esta ley. • Se sugiere que en el artículo 27 se integre al Consejo de la Judicatura. • En el artículo 29, 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. • En el artículo 39, 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. • Sugieren crear una nueva disposición general, debido a que el Ministerio de Finanzas deberá asignar los recursos necesarios a cada una de las instituciones para la implementación operativa de las atribuciones conferidas. • Sugieren crear una nueva disposición transitoria. El Consejo de la Judicatura conjuntamente con la Fiscalía General del Estado deberán, en el término de 60 días, estructurar un catálogo de delitos digitales.
Diego Álvarez, country manager-Niubox Legal Digital S/O, 6 de febrero de 2024	Presenta observaciones puntuales al proyecto de ley, entre las que se pueden resaltar las siguientes: Es adecuada la creación del sistema nacional de seguridad y, a su vez, el de un ente único como competente en la materia, en este caso Mintel. Esto, en virtud de que es necesario crear infraestructura específica que trate con seguridad digital. A su vez, esta normativa debe ser lo suficientemente flexible y general para evitar que la misma resulte inadecuada u obsoleta ante nuevas modalidades de ataques cibernéticos. Es necesario que esta ley se base en principios abiertos que puedan adaptarse a los diferentes riesgos cibernéticos ya que los mismos varían y cambian de forma exponencial. Por ende, tener normativa muy específica podría dejar a la misma obsoleta. Por ello, es adecuada la delegación al sistema nacional de creación de políticas específicas. El mismo debe procurar ser claro y preciso. • Es necesario crear un centro especializado para la identificación y manejo de riesgos y ataques cibernéticos.

Remitente Fecha documento	Síntesis de observaciones
	Para ello se recomienda: ○ Fortalecer el rol del Ecucert y brindarle atribuciones a nivel nacional, de apoyo para entes públicos y privados y no solo específico para las redes de telecomunicaciones. ○ Crear un centro específico para estos incidentes. El mismo, nuevamente, debería receptar y mitigar riesgos cibernéticos reportados por las instituciones nacionales. ○ Independientemente de la figura de institución que se adopte, el mismo debe operar a nivel nacional, transversal y multisectorial para identificar y mitigar riesgos y ataques cibernéticos. Es imprescindible mencionar la importancia del levantamiento y control estadístico de ciberataques en el Ecuador en el marco de la ley. • Armonización de leyes: con la finalidad de garantizar la seguridad jurídica para los ciudadanos e instituciones, es necesario que esta nueva ley tome en cuenta leyes que ya hacen referencia al tema y a partir de ello reformar o incorporar sus disposiciones. Es imprescindible evitar inconcordancias para que esta ley sea plenamente ejecutable. Estas son: ○ Ley de Transformación Digital y su reglamento ○ Ley de Telecomunicaciones ○ Ley Orgánica de Datos Personales. • En el caso específico de esta ley, el artículo 43 obliga al responsable del tratamiento de notificar la vulneración de la seguridad de datos personales a la autoridad de Protección de Datos Personales y la Agencia de Regulación y Control. ○ Reglamento a la Ley de Datos Personales: el capítulo VI sobre la vulneración de seguridad a los datos personales. Se destacan los siguientes artículos: • El artículo 24 obliga al responsable de datos personales a notificar cuando haya una vulneración de seguridad a la autoridad de datos y al Arcotel. Además, establece las causales mediante las cuales se entiende que hay una vulneración de seguridad. 1. Cuando los datos fueron destruidos, ya no existen o no están disponibles de una forma que sea de utilidad para el responsable del tratamiento; 2. Cuando los datos personales han sido alterados, corrompidos o dejan de estar completos; 3. Cuando el responsable del tratamiento ha perdido el control o el acceso a los datos, o ya no obran en su poder; o, 4. Cuando el tratamiento no ha sido autorizado o es ilícito, lo cual incluye la divulgación de datos personales o el acceso por parte de destinatarios que no están autorizados a recibir o acceder a los datos o

Remitente Fecha documento	Síntesis de observaciones
	cualquier otra forma de tratamiento que se ejecuta contrariando las disposiciones de la ley. • La finalidad de estas notificaciones, según el artículo 25, son para un registro estadístico, por lo que es necesario armonizar e identificar a una sola entidad esta competencia para evitar una duplicidad de obligaciones y aumento de carga burocrática. • El artículo 31, además, establece evaluaciones de impacto en ciertos casos que deben ser presentados ante la autoridad. Nuevamente, es necesario evitar duplicidad de trámites. o Políticas emitidas por el Mintel. • Ejemplos incluyen la estrategia de ciberseguridad que delimita ciertos parámetros y principios para este fin. Nuevamente, la finalidad es que la Ley de Seguridad Digital armonice estos conceptos ya previamente identificados. o Código Orgánico Integral Penal. • En línea con lo previamente dicho, es necesario armonizar y brindar claridad sobre los requisitos y procesos clave mediante los cuales las instituciones sujetas a la regulación deberán cumplir. Esto incluye: o Una identificación clara de autoridades, su rol y competencias. o Evitar duplicidades. Ejemplos, incluyen el artículo 43 de la LOPD, pues se genera una confusión para el sujeto regulado y una doble carga. • Incentivar la resiliencia cibernética. El reporte de incidentes es sumamente importante para tomar acción. Sin embargo, es necesario enfocarnos, además, en la estrategia que se tomará posterior al reporte de incidentes. Nuevamente, estos temas específicos pueden ser desarrollados por el comité o sistema nacional de seguridad digital. • Adopción de estándares internacionales y cooperación internacional: los crímenes cibernéticos pueden ser transfronterizos, y en la mayoría de los casos lo son. Por ende, es necesario no solo impulsar la cooperación internacional con otros Gobiernos y organizaciones públicas, privadas y no gubernamentales, sino que buscar una armonización cada vez más global de estándares y normativa internacional. • Adopción de tecnologías emergentes para garantizar la seguridad digital. Es primordial que esta ley incentive la adopción de nuevas tecnologías para combatir el ciberterrorismo y ataques cibernéticos con la finalidad de salvaguardar la información ciudadana. Ejemplos de éxito incluyen países como Costa Rica y Estonia, mismos que tienen una dependencia cibernética en operadoras de nube pública internacionales para asegurar

Remitente Fecha documento	Síntesis de observaciones
	la información de sus instituciones y ciudadanos.
Diego Urbina, gerente de Región Sur de Amazon Web Services S/O, 08 de febrero de 2024	Presenta observaciones a 16 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • El ámbito de aplicación se encuentra muy amplio por lo que se recomienda delimitar. 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, entendido como un dominio y componente del territorio ecuatoriano, donde las vulneraciones a los activos digitales y sus afectaciones en el entorno físico, pueden atentar contra la ciudadanía y el Estado. (...). • Garantizar el acceso a la verdad de los hechos en el ciberespacio es una labor que podría llegar a ser inejecutable para el Estado, ya que se necesitaría una amplia infraestructura y capacidad técnica y operativa para determinar las falsedades, los responsables y mecanismos que garanticen el acceso. Esto puede desembocar en acciones contra el Estado por incumplimiento. Artículo 3. Finalidades de la Ley. Son finalidades de esta ley: (...). 8. Fomentar una cultura de la ciberseguridad responsable en la ciudadanía, mediante el desarrollo de capacidades en seguridad digital. No se establece en la ley quiénes son los emisores de datos, además que es virtualmente imposible que el Estado garantice la identificación relativa al tráfico de los datos. Adicionalmente, no se realiza una distinción entre encargados y responsables de datos. Esto puede acarrear conflictos para garantizar la disponibilidad de información y preservación de datos, así como la obligación de garantizar el acceso a la verdad de los hechos. Artículo 4. Principios. La aplicación de la presente ley se rige por los principios previstos en la Constitución de la República, los instrumentos internacionales vigentes en Ecuador y los siguientes principios específicos: a) Eliminar principio. b) 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 información para la determinación de los hechos referentes a vulneraciones dentro de dicho espacio. • Dentro de las definiciones debería diferenciarse a los

Remitente Fecha documento	Síntesis de observaciones
	titulares de los datos de los emisores de datos. Así mismo, debe incluirse definiciones de los responsables y encargados de los datos, en línea con la Ley Orgánica de Protección de Datos. En principios, no hay definiciones claras de a quiénes se está protegiendo. No se define quiénes son los proveedores del servicio, los responsables y las competencias que se tiene. En cuanto a la auditoría de ciberseguridad se debe establecer el tiempo del estudio periódico y la autoridad encargada de recibirlos. La definición de infraestructura crítica, digital y estratégica son demasiado abiertas al igual que el alcance de servicios esenciales. Esto es importante por la protección especial que se establece en los artículos siguientes. Se sugiere utilizar las definiciones del marco NIST https://csrc.nist.gov/glossary/term/critical_infrastructure. En cuanto a la definición de proveedor de servicios, se sugiere eliminar la definición, pues es demasiado general. No todo proveedor de servicios está sujeto a esta ley. La ley aplica a los proveedores de servicios esenciales y ya se cuenta con una definición para dichos servicios. Artículo 5. Definiciones. En la aplicación de la presente Ley se observarán las siguientes definiciones: c. Auditoría de ciberseguridad. Es el estudio periódico anual 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. Infraestructura crítica. Sistemas y activos, ya sean físicos o virtuales, tan vitales para el Estado que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud o seguridad pública nacional, o cualquier combinación de esas cuestiones. 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 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. Servicios críticos para el funcionamiento y bienestar de la sociedad y la economía, cuya interrupción o compromiso podría tener graves consecuencias como, por ejemplo: electricidad, gas y petróleo; suministro y tratamiento de agua; hospitales, emergencias médicas y laboratorios; aeropuertos, ferrocarriles, puertos y tráfico vial; bancos, bolsas de valores y sistemas de pago: y servicios gubernamentales esenciales, defensa y administración pública. Proveedor de servicios. Eliminar esta definición. Responsable de datos. Se refiere a la

Remitente Fecha documento	Síntesis de observaciones
	persona física o jurídica, autoridad pública, agencia u otro organismo que es responsable de la seguridad de la información en una organización. Es decir, es la persona o entidad que toma las decisiones sobre la seguridad de la información, incluyendo la evaluación de riesgos, la implementación de medidas de seguridad, la gestión de incidentes y la supervisión del cumplimiento normativo. Encargado de datos. Se refiere a la persona física o jurídica, autoridad pública, agencia u otro organismo que realiza tareas de seguridad de la información en nombre del responsable de la seguridad. Es decir, es la persona o entidad que lleva a cabo las medidas de seguridad implementadas por el responsable, siguiendo sus instrucciones y con los fines establecidos por este. • Se debe especificar el mecanismo o forma de protección de este tipo de infraestructuras. Artículo 7. Infraestructura crítica, estratégica y servicios esenciales. Se protege las infraestructuras críticas y estratégicas del sector público o privado (...). El reglamento a la ley establecerá los mecanismos de protección, así como el alcance de los servicios esenciales sujetos a dicha protección. • De igual manera, se debe determinar cuáles son y a qué se refiere con los activos de información de alto impacto y especificar los mecanismos o formas de protección. Se recomienda que las clasificaciones estén lincadas a normativa internacional, en este caso ISO 27001. Artículo 8. Activos de información de alto impacto. (...). El Reglamento a la ley establecerá el mecanismo de protección y clasificación de los activos en general. • No se establece quién es el encargado de la respuesta a incidentes digitales, si es el responsable de datos, el titular o la autoridad. Tampoco se determina con claridad ante quién se realizaria la denuncia y quién seria el responsable de la investigación (nuevamente: el responsable de datos, la autoridad competente). Artículo 24. Respuesta a incidentes digitales. La gestión integral de incidentes en el ciberespacio u otros entornos digitales es competencia exclusiva del Centro de Respuestas a Incidentes de Seguridad Digital integrando, (...). La identificación, detección, análisis, evaluación y notificación de incidentes, así como la contención y neutralización, en los ámbitos de ciberdefensa, ciberseguridad ciudadana, ciberinteligencia y ciberdiplomacia, se gestionará de manera integral e intersectorial, a través de subsistemas en virtud de lo establecido en el artículo 41 de la presente ley. • Se debe especificar quiénes son los responsables de la recuperación. Si son los responsables de datos, las autoridades, etcétera. Artículo 25. Recuperación ante incidentes digitales. (...). Será coordinado y articulado a

Remitente Fecha documento	Síntesis de observaciones
	través del Centro de Respuestas a Incidentes de Seguridad Digital, previa aprobación de protocolos por parte del Comité Nacional de Seguridad Digital de acuerdo con el nivel y tipo de incidente. • Las certificaciones pueden ser una carga burocrática para las instituciones responsables. Adicionalmente, existen estándares internacionales que pueden ser utilizados en lugar de crear nuevas certificaciones que deban estar actualizándose constantemente para no caer en caducidad. Sobre todo, en temas de tecnología, en donde existen constantes cambios y avances. Artículo 34. Atribuciones del Comité Nacional de Seguridad Digital. El Comité Nacional de Seguridad Digital tendrán las siguientes atribuciones: 17. Aprobar la normativa correspondiente para garantizar el cumplimiento de estándares internacionales de seguridad digital. 21. Incentivar el cumplimiento de normas, estándares internacionales, esquemas voluntarios; y la creación de incentivos de mercado y otras iniciativas para aumentar la confianza digital; (...). • Las acreditaciones pueden ser una carga burocrática para la institución responsable. En otro tipo de normativas se ha cambiado incluso por controles expost para que no se termine en un cuello de botella que genere que la operación de los prestadores de servicios se vea paralizado. Artículo 68. Acreditaciones a operadores, proveedores y sistemas de información y comunicaciones. El Instituto Ecuatoriano de Normalización o su equivalente acreditará el cumplimiento de normativa técnica nacional y estándares internacionales (...). • Las certificaciones pueden ser una carga burocrática para las instituciones responsables. Adicionalmente, existen estándares internacionales que pueden ser utilizados en lugar de crear nuevas certificaciones que deban estar actualizándose constantemente para no caer en caducidad. Sobre todo, en temas de tecnología en donde existen constantes cambios y avances. Artículo 69. Estándares internacionales de seguridad digital. El cumplimiento de estándares internacionales en materia de protección de datos y seguridad digital son instrumentos que permiten tener un factor crítico de cumplimiento para un producto, servicio o proceso en materia de seguridad digital. Los procedimientos para acreditar dicho cumplimiento se establecerán en el Reglamento de la presente Ley. El cumplimiento de los estándares internacionales de seguridad digital y protección de datos, generarán acciones afirmativas y acceso preferencial a beneficios cuando corresponda y estarán orientadas a promover las buenas prácticas de seguridad digital. • Se debe establecer cuáles son los ejercicios de seguridad

Remitente Fecha documento	Síntesis de observaciones
	digital o lineamientos generales que hagan que el texto sea menos obscuro, ya que de la manera que está redactado podría causar discrecionalidades en su establecimiento. Adicionalmente, se podría establecer una periodicidad para no dejar tan abierto el artículo. Artículo 72. Ejercicios de seguridad digital. Los ejercicios de seguridad digital son simulacros de vulneraciones que tienen como objetivo fortalecer las capacidades para preservar la seguridad digital del Estado. Se realizarán de manera anual en instituciones públicas y se desarrollarán según el reglamento que el comité de seguridad digital apruebe para el efecto. • De acuerdo con la disposición reformatoria cuarta del proyecto, la Superintendencia de Datos Personales debe enviar informes trimestrales de riesgos, incidentes y ataques informáticos al rector del sistema (dentro de nuestra propuesta al rector del comité). Así, se puede establecer la base del catálogo para lo cual también debería establecerse un responsable mediante reglamento. Artículo 73. Catálogo de incidentes. El catálogo es un repositorio de incidentes generados con base en los informes trimestrales de riesgos, incidentes y ataques informáticos presentados por la Autoridad Nacional de Datos Personales al ente rector del Comité Nacional de Seguridad Digital. (...) Su funcionamiento y rectoría será establecido mediante Reglamento de esta Ley. • Analizar el alcance de este artículo. Artículo 75. Derecho a acceder a la información para la determinación de los hechos. Las personas tienen derecho a acceder a la información para determinar los hechos referentes a vulneraciones en el ciberespacio, a través de la coordinación del Comité Nacional de Seguridad Digital y del Subsistema de Ciberseguridad Ciudadana, (...). • El acceso a la verdad de los hechos tiene limitaciones. Se debe revisar el alcance del artículo. Artículo 76. Mecanismos para la determinación de los hechos. (...) acceso a la información para determinar los hechos referentes a vulneraciones en el ciberespacio, (...). • Se debe especificar en la ley que hay que crear mecanismos de control y transparencia mediante el reglamento a la ley, para evitar posibles temas de corrupción en el manejo del fondo. Artículo 79. Fondo para la seguridad digital, seguridad sistémica y acceso a la información para la determinación de los hechos. Sin perjuicio de las asignaciones adicionales que tenga el Comité Nacional de Seguridad Digital y los subsistemas, su funcionamiento, las políticas públicas de ciberseguridad ciudadana, seguridad sistémica y acceso a la información para la determinación de los hechos

Remitente Fecha documento	Síntesis de observaciones
	referentes a vulneraciones en el ciberespacio, así como la aplicación de los instrumentos creados por esta Ley, se financiarán mediante el Fondo para la Ciberseguridad, cuya creación, rectoría y mecanismos de control y transparencia serán establecidos en el Reglamento a la Ley.
Magíster Diana Carolina Velasco Aguilar, directora nacional de Registros Públicos Oficio Nro. DINARP-DINARP-2024-0041-OF. De 29 de enero de 2024	Presenta observaciones a 17 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 1, la observación propuesta sugiere que, para el ejercicio de un sistema nacional de seguridad digital, se debe tener en consideración que existe el plan de ciberseguridad y de la estrategia nacional de ciberseguridad, entre otras. Con el fin de evitar antinomias normativas, es necesario verificar su alcance constitucional. Se recomienda reemplazar seguridad del Estado por seguridad digital del Estado, puesto que se está regulando aspectos digitales. • En el artículo 4, es pertinente sugerir que en relación al principio de integridad; el Comité Nacional de Seguridad Digital, tenga entre sus funciones definir el esquema del ciclo de vida del dato, ya que este puede variar dependiendo el sector al cual esté dirigido. Por ejemplo, en el sistema nacional de registros públicos existe una interconexión de los registros, lo que implica un intercambio de información dinámica que puede no ocurrir en otros sectores. Considerar definir el ciclo de vida del dato entre las atribuciones del Comité Nacional de Seguridad Digital. (Artículo 32-38). En el artículo 5, considerar definir los siguientes términos: Riesgo. Situación o circunstancia no deseable que tiene tanto una probabilidad de que ocurra y una consecuencia potencialmente negativa. Riesgo de ciberseguridad. Un riesgo de ciberseguridad son las probabilidades de que una amenaza se materialice y la información, datos personales o el acceso a cuentas bancarias queden expuestas o sean modificadas por personas no autorizadas. • En el artículo 18, se sugiere reemplazar "en aplicación de la ley" por "en aplicación de la presente Ley". Se recomienda que el segundo párrafo se desarrolle como un artículo individual a efectos de que se cumpla en su totalidad el objetivo de enfoque de derechos digitales, considerando que el particular ya se encuentra normado en el artículo 77 de la Ley Orgánica de Telecomunicaciones. Artículo 77, Ley Orgánica de Telecomunicaciones. Interceptaciones. • En el artículo 19, se sugiere hacer énfasis este enfoque, al momento de reglamentar los procedimientos y mecanismos para la preservación, restauración de estructuras y funciones.

Remitente Fecha documento	Síntesis de observaciones
	• En el artículo 22, se recomienda que se defina qué entidad se encargará de emitir los lineamientos para los análisis de gestión de riesgos, considerando que la presente ley aplica para entidades públicas y privadas. Actualmente las entidades de la Función Ejecutiva tienen implementado el esquema de seguridad de la información, que es elaborado y puesto a disposición de las mentadas entidades por Mintel. Se recomienda de igual manera considerar el artículo 38 de la Ley Orgánica de Protección de Datos Personales, que hace referencia al mecanismo gubernamental de seguridad de la información. • En el artículo 23, se recomienda realizar énfasis en el presente artículo al momento de reglamentar: La implementación de procesos de identificación, análisis, evaluación y catalogación de activos de información frente a vulnerabilidades, amenazas y riesgos dentro del sector privado. Se recomienda, entre las competencias del Comité Nacional de Seguridad Digital, sea el implementar análisis de gestión de riesgos, para estos efectos. • En el artículo 26, se sugiere tener en cuenta la constitucionalidad de crear un sistema nacional mediante ley. • En el artículo 27, se sugiere: Artículo 27. Integración del Sistema Nacional de Seguridad Digital. El Sistema Nacional de Seguridad Digital estará integrado por las siguientes instituciones y organismos: (...). 15. La Autoridad de Protección de Datos Personales; 16. Las superintendencias del país; (...). • En el artículo 33, en atención a las competencias de la Dirección Nacional de Registros Públicos (Dinarp), en su calidad de ente rector del sistema nacional de registros públicos, se recomienda verificar la pertinencia de incluirla como parte del comité. La Dirección Nacional de Registros Públicos como entidad encargada de administrar el sistema nacional de registros públicos, es la encargada de interconectar la información y los datos inscritos y registrados, siendo importante la incorporación de la Dinarp con el afán de procurar una coordinación adecuada para el cumplimiento de las funciones del comité. • En el artículo 39, se recomienda revisar una posible antinomia respecto a las competencias con las asignadas al Ecucert (Centro de Respuesta a Incidentes informáticos del Ecuador), a cargo de Arcotel, como su objetivo y funcionalidad. • En el artículo 43, se recomienda verificar la armonía normativa con las disposiciones inherentes a ciberseguridad y ciberdefensa, previstas en la Ley Orgánica para la Transformación Digital y Audiovisual.

Remitente Fecha documento	Síntesis de observaciones
	• En el artículo 51, se recomienda especificar el alcance normativo respecto a los funcionarios públicos y en qué consistirá, de igual manera lo definido como "integrará" ante organizaciones internacionales, así como la pertinencia de la expresión "u otras". • En el artículo 75, se recomienda especificar la definición de daño objetivo, con el fin de evitar interpretaciones eventualmente contradictorias. • En las disposiciones generales, se recomienda revisar la concordancia y alcance con los diferentes cuerpos normativos como: o Ley Orgánica de Transparencia y Acceso a la Información Pública. o Ley Orgánica de la Función Legislativa o Comisión de Fiscalización y Control Político (respecto a sus competencias). • En la disposición reformatoria cuarta, se recomienda, respecto a la periodicidad, se exija la presentación del informe de manera semestral. Tomando como consideración que los incidentes de seguridad identificados toman tiempo en ser gestionados y subsanados, por consiguiente, tres meses no es un lapso suficiente para determinarlos. • En la disposición transitoria primera, se recomienda ampliar el plazo para la expedición del reglamento a 180 días, considerando que es un plazo razonable para que la Presidencia coordine su elaboración y cumpla con su puntual expedición.
Magister Javier Andrés Borja Ortiz, abogado y experto en Ciberseguridad S/O, de 21 de febrero de 2024	Presenta observaciones a 32 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: En el artículo 4, se sugiere cambiar en el principio de disponibilidad la palabra ataques por "ciberataques"; así como en toda la ley realizar el cambio. • En el artículo 5, se sugiere incluir lo marcado: 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 perpetrar un delito. 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 digital e información estratégica del Estado, así como apoyar el cumplimiento de operaciones para la defensa de la soberanía y la integridad territorial. 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 digital, estratégica o servicio esencial que, a su vez, pone en riesgo la vida o la salud de muchas personas, provoca

Remitente Fecha documento	Síntesis de observaciones
	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. • Se sugiere crear un nuevo capítulo donde se haga referencia a los derechos de libertad en entornos digitales: Capítulo III. Derechos de libertad en entornos digitales. Sección primera. Derechos de libertad en el entorno digital. Artículo 6. Derechos y libertades en entornos digitales. Los derechos y libertades reconocidos en la Declaración Universal de Derechos Humanos, la Constitución de la República de Ecuador, la Convención Americana de Derechos Humanos, Pacto Internacional de Derechos Civiles y Políticos y los tratados y acuerdos internacionales legalmente ratificados son aplicables en los entornos digitales. En los procesos de transformación digital; el desarrollo y el uso de la tecnología digital; implementación de instrumentos para la reducción, respuesta y recuperación ante riesgos, amenazas e incidentes digitales; expedición de regulaciones y normas técnicas por las entidades de rectoría, regulación, coordinación, supervisión y control; ejercicios de seguridad digital; recopilación de información para el repositorio de incidentes generados en el sistema nacional de seguridad digital; entre otros, se garantizará la dignidad, los derechos fundamentales, el libre desarrollo de la personalidad, el logro del bien común y la neutralidad de la red. Artículo 7. Cumplimiento normativo en entornos digitales. El principio de cumplimiento normativo se declara que es de aplicación plenamente al desarrollo de los entornos digitales, por tanto, los desarrollos científicos, tecnológicos y demás, contemplarán en la determinación de sus requerimientos el cumplimiento de este principio. Sección segunda. Derechos de identidad en el entorno digital. Artículo 8. Derecho a la identidad en el entorno digital. El derecho a la propia identidad será exigible en el entorno digital. Determinada por el nombre y por demás elementos que la configuran según como lo instituye la normativa nacional e internacional, misma que debe garantizar el derecho a la gestión de la identidad propia, sus atributos y acreditaciones. La identidad no podrá ser controlada, manipulada o suplantada por terceros contra la voluntad de tu titular. Artículo 9. Garantía de verificación de identidad. El Estado garantizará una verificación de la identidad en el entorno digital segura, evitando manipulaciones, suplantaciones o control por parte de terceros sin previo consentimiento. De igual manera, cerciorará la provisión y utilización de medios digitales para la acreditación de la identidad. Sección tercera. Derechos a la protección de datos. Artículo 10. Principios

Remitente Fecha documento	Síntesis de observaciones
	para la protección datos personales. La Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, la Ley Orgánica de Seguridad Digital, reconocen el derecho a la protección de datos de carácter personal. El tratamiento de datos personales se regirá por los principios de juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización de datos personales, confidencialidad, calidad y exactitud, conservación, seguridad, responsabilidad proactiva y demostrada, aplicación favor al titular, independencia de control. Artículo 11. Derecho a la información en el entorno digital. Toda persona tiene derecho a ser informada en el momento de la recolección de datos; los fines del tratamiento, los tipos de tratamiento; tiempo de conservación. Así también mantiene el derecho de acceso, rectificación, actualización, actualización y oposición; derecho a la portabilidad; derecho a la suspensión del tratamiento; derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas; derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas; derecho a la educación digital, en los términos previstos por la normativa especial de protección de datos y el reglamento a la presente ley. Artículo 12. Protección de derechos digitales. El cumplimiento de los derechos descritos en el artículo precedente, estará sujeto al control de la autoridad de Protección de Datos y demás organismos competentes en materia de protección de datos. • En el artículo 7, cambiar "se protege" por "el Estado a través de sus instituciones protegerá". Incluir al final del texto: "para lo cual se desarrollará un catastro nacional de infraestructura crítica digital conforme al reglamento a la presente ley". • En el artículo 8, 9 y 10, cambiar "se protege" por "el Estado a través de sus instituciones protegerá". • En el artículo 11, se sugiere el siguiente texto: Artículo 18. Diplomacia en el ciberespacio. El Estado a través de sus instituciones protegerá y fomentará 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, riesgos e incidentes digitales que son transnacionales y requieren ser abordados a través de la cooperación internacional, el fortalecimiento de la confianza y la seguridad internacional. Se sugiere ajustar en todo el texto de la ley lo siguiente: amenazas, riesgos e incidentes digitales. • En el artículo 12, cambiar "se protege" por "el Estado a través de sus instituciones protegerá". En el artículo 12

Remitente Fecha documento	Síntesis de observaciones
	se sugiere suprimir el (;). Artículo 12. Cultura de ciberseguridad. (...). Toma de medidas preventivas y de respuesta; resiliencia digital. Se sugiere el texto siguiente: Artículo 19. Cultura de ciberseguridad. El Estado a través de sus instituciones protegerá y fomentará 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 amenazas, riesgos e incidentes digitales, 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 prospección y anticipación estratégica, promoción de la ética y el pensamiento crítico de las personas en el entorno digital. • Se sugiere cambiar el título del capítulo por principios específicos de la seguridad digital. • Se sugiere el siguiente texto: Artículo XX. Principio de planificación estratégica. La seguridad digital se orientará por el Plan Nacional de Seguridad Digital, el Plan Nacional de reducción, respuesta y recuperación ante riesgos, amenazas e incidentes digitales, los planes específicos de defensa y seguridad pública y ciudadana; así como, la Estrategia Nacional de Seguridad Digital (...). • En el artículo 20, incluir la palabra digitales después de incidentes. (...) incidentes digitales (...). • En el artículo 22, se sugiere incluir la palabra digitales después de incidentes. (...) incidentes digitales (...). • En el artículo 26, se sugiere cambiar el capítulo I por: Integración, organización y funciones del sistema nacional de seguridad digital. Ajustar con mayúscula las primeras letras de política de seguridad digital. Ajustar el segundo párrafo por lo siguiente: El sistema nacional de seguridad digital tiene por fin promover la seguridad digital mediante la prevención, gestión e investigación de las amenazas, riesgos, incidentes digitales y ciberdelitos que afecten a la seguridad integral en entornos digitales y al ejercicio de los derechos digitales y libertades de sus ciudadanos en el ciberespacio, los sistemas informáticos y la red. • En el artículo 29, 1. En el artículo 29 numeral 9, incluir al final lo siguiente: 9. Cumplir las disposiciones, directrices, normas técnicas, lineamientos expedidos por las entidades de rectoría, gestión y coordinación, en función de sus competencias. En el numeral 10, se recomienda incluir una transitoria con la frase: Las entidades privadas que conforman el sistema nacional de seguridad digital tendrán el plazo de 5 años para iniciar el proceso de designación obligatoria de un oficial

Remitente Fecha documento	Síntesis de observaciones
	responsable de ciberseguridad. La entidad rectora en materia de educación superior fomentará la creación de carreras de pregrado relacionadas con esta temática, a fin de solventar la futura demanda de profesionales en este sector. En el numeral 11, se sugiere el siguiente texto: 11. Entregar la información requerida por las entidades de rectoría y regulación, necesaria para garantizar la seguridad digital; y, en el caso de información que esté sujeta a reserva legal la petición estará debidamente fundamentada y justificada, previo acuerdo de confidencialidad. • En el artículo 31 numeral 23, se sugiere cambiar la expresión banco de alertas por bases de datos, o bases de conocimiento, debido a que el término banco de alertas no está definido. En el numeral 25. Elaborar estrategias y protocolos para garantizar la seguridad digital (...). • En el artículo 32, se sugiere ajustar el texto por: El comité nacional seguridad digital es el organismo estratégico, colegiado, de coordinación, transversalización, evaluación de 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 e incidentes digitales, ciberataques o crisis que se puedan dar en el ciberespacio. • En el artículo 33 numeral 1, incluir lo siguiente: 1. La máxima autoridad del ente rector del sistema de seguridad digital quien lo presidirá y gozará de voto dirimente; (...). • En el artículo 36, se sugiere incluir lo siguiente: Artículo 36. Secretaría del Comité Nacional de Seguridad Digital. 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 periodo de dos años, renovable por una sola vez. El reglamento determinará las áreas de conocimiento y experiencia que debería acreditar el secretario. • Se sugiere ajustar el artículo 38 por lo siguiente: 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 de este sistema, con el Sistema Nacional de Seguridad Digital. • Se sugiere incluir en el artículo 41. Gestión integral e intersectorial de respuesta a incidentes digitales. La respuesta a incidentes digitales se gestionará de manera integral e intersectorial, a través de los subsistemas que se encargarán, de acuerdo al ámbito de sus

Remitente Fecha documento	Síntesis de observaciones
	competencias, de la detección, análisis, evaluación y notificación de incidentes al centro nacional de respuesta a incidentes de seguridad digital; así como, la contención y neutralización, en los ámbitos de ciberdefensa, ciberseguridad, ciberinteligencia y ciberdiplomacia. • Se sugiere ajustar el artículo 43 lo siguiente: Artículo 43. Ente ejecutor de la política de ciberdefensa. El ente rector de la Defensa Nacional (...). • En el artículo 44 se sugiere completar: (...). 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 Nacional del Seguridad Digital y ente rector del Sistema Nacional de Seguridad Digital; (...). 16. Elaborar un registro de las evaluaciones realizadas y presentarlo anualmente al ente rector del Sistema Nacional de Seguridad Digital; (...). 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 digitales, ciberataques y crisis en el ciberespacio que puedan poner en riesgo la soberanía, la integridad territorial, los recursos estratégicos y la seguridad del Estado; y, suscribir los acuerdos y convenios interinstitucionales en el ámbito de sus competencias; (...). • Se sugiere ajustar e incluir en el artículo 45 del subsistema de ciberseguridad. El subsistema de ciberseguridad articulará y coordinará acciones con el sistema nacional de inteligencia, la entrega de información clasificada de conformidad con la ley. El subsistema de ciberseguridad establecerá mecanismos para la garantía del acceso a la información verificada para determinar la verdad de los hechos, la no repetición y la no impunidad. 2. Elaborar el componente de ciberseguridad para la prevención, investigación y combate a la ciberdelincuencia para su incorporación en el plan nacional de seguridad digital, el plan nacional de reducción, respuesta y recuperación ante riesgos, amenazas e incidentes digitales y la estrategia nacional de seguridad digital; 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 Nacional de Seguridad Digital y el 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

Remitente Fecha documento	Síntesis de observaciones
	reducción, respuesta y recuperación frente a amenazas, riesgos, incidentes digitales, 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 anualmente; 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 del Ecuador; 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, nacionales 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 del Ecuador 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, entre otros. • Se sugiere el siguiente ajuste en el artículo 48. Subsistema de ciberinteligencia. El subsistema de ciberinteligencia, (...). El subsistema de ciberinteligencia tendrá coordinación directa con el subsistema de ciberdefensa, el subsistema de ciberseguridad y el 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 digital y del centro nacional de respuesta a incidentes de seguridad digital, así como otras entidades que deban entregar información en función de sus competencias, a fin de contar con información para la identificación, alerta y respuesta ante amenazas, riesgos e incidentes digitales, contra la infraestructura estratégica, infraestructura crítica digital, los servicios esenciales o la seguridad ciudadana. • En el artículo 50, se sugiere incluir el siguiente numeral (...) 3. Establecer las directrices y acreditar los sistemas de información y comunicaciones; (...). • Se sugiere los siguientes ajustes en el artículo 51. Subsistema de ciberdiplomacia. El subsistema de ciberdiplomacia, estará conformado por el ente rector en materia de relaciones exteriores y movilidad humana, el

Remitente Fecha documento	Síntesis de observaciones
	ente rector en materia de comercio exterior, e integrará a los funcionarios públicos acreditados (...). El Subsistema de ciberdiplomacia tendrá coordinación directa con el subsistema de ciberdefensa, el subsistema de ciberseguridad 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 digitales; (...). • Se sugiere ajustar el artículo 54, remplazar ministerio por ente, en razón de que puede cambiar la naturaleza de ministerial. • Se sugiere ajustar el artículo 57, se sugiere lo siguiente en el numeral 9, registrar las denuncias a escala nacional por delitos informáticos y presentar reportes semestrales al ente rector del sistema nacional de seguridad digital y del Comité Nacional de Seguridad Digital; (...). • Se sugiere ajustar en los siguientes numerales del artículo 59: 2. Definir e implementar planes, programas y proyectos para el mejoramiento de las capacidades de seguridad digital, de conformidad con los lineamientos y directrices del Comité Nacional de Seguridad Digital (...). 1. Proponer al Comité Nacional de Seguridad Digital, (...). • Se sugiere ajustar en el artículo 60 lo siguiente: 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 Nacional de Seguridad Digital y precautelando los criterios de clasificación de la información. 3. Establecer, dirigir, orientar y coordinar la implementación de la Estrategia Nacional de Seguridad Digital de la institución de la que forma parte; (...). • Se sugiere que se elimine la disposición general segunda y en su lugar se incluya una nueva disposición reformatoria con el siguiente texto: Agréguese en la Ley de Seguridad Pública y del Estado, en su artículo 24, del control. El siguiente párrafo al final del articulado: La entidad rectora del sistema nacional de seguridad digital, en sesión reservada semestral, rendirá cuentas ante la Asamblea Nacional a través de la comisión responsable de la temática de seguridad.
Magíster Bolívar Wladimir Tello Astudillo, director general ECU-911 Oficio Nro. SIS-SIS-2024-0072-OF, de 25 de enero de 2024	Presenta observaciones a 13 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 4, se recomienda cambiar el nombre del principio de reserva de la información por confidencialidad (conforme a la figura Nro. 1, principios de la S.I. Nota: Para leer figura, ver Registro Oficial Suplemento 228 de 10 de enero de 2020, página 13, para la debida concordancia con el Acuerdo Ministerial 25

Remitente Fecha documento	Síntesis de observaciones
	esquema gubernamental de seguridad de la información EGSI. También, en propuesta de definición reserva de la información modificar el texto eliminando las comas innecesarias: (...) de investigaciones que realicen las autoridades públicas competentes sobre violaciones (...). • En el artículo 5, se sugiere lo siguiente: 1) Se sugiere que las definiciones se establezcan en orden alfabético. 2) Se sugieren cambios en las siguientes definiciones: Auditoría de ciberseguridad. Es el estudio periódico de cumplimiento para determinar la garantía de ciberseguridad a la que se someterán las y los sujetos, redes, infraestructuras y sistemas que determine la presente ley. Ciberdelito. Conducta típica, antijurídica y culpable 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. 3) Se sugiere incluir la siguiente definición: Vulnerabilidad. Constituye la omisión cambiar o anomia por o anomalía detectada en 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. 4) Deberían definirse también los términos: infraestructura crítica; infraestructura estratégica; y, servicios esenciales, a fin de facilitar la interpretación y aplicación por parte de los ciudadanos y demás personas que no posean conocimientos técnicos sobre la materia. • Deben corregirse los verbos usados en un contexto plural, pues se están escribiendo en singular: Se protegen; se fomentan; se defienden, etcétera, en los artículos, 7, 8, 9, 10, 11, 12. • En el artículo 16, se sugiere modificar el artículo por el siguiente texto: Acorde al 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. • Se sugiere en el artículo 26, que el sistema nacional de seguridad digital tiene como finalidad 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

Remitente Fecha documento	Síntesis de observaciones
	Estado y al ejercicio de los derechos y libertades de sus ciudadanos en el ciberespacio, los sistemas informáticos y la red. • En el artículo 27, se sugiere lo siguiente: 1. Se sugiere cambiar el nombre del Sistema Integrado de Seguridad ECU-911 o quien haga sus veces; por lo siguiente: 1) El Servicio Integrado de Seguridad ECU-911 o quien haga sus veces. 2) Así mismo, se sugiere cambiar el numeral 18 por lo siguiente: 18. Las entidades públicas y privadas que administren, operen o proveen infraestructura crítica, estratégica o servicios esenciales. • En el artículo 29, conforme al desarrollo de las actividades establecidas en los diferentes instrumentos para su ejecución, se recomienda la creación del área específica en seguridad digital por institución, con la finalidad de mantener el control sobre el uso y manejo de los activos de información, a través de una estructura autónoma de las demás unidades para aplicar la normativa gubernamental como propia de la entidad. En el reglamento se incorpore las directrices específicas para la creación de las unidades de seguridad digital en cada institución, a fin de gestionar de manera oportuna y fortalecer el sistema nacional de seguridad digital. • En el artículo 45, debido a la naturaleza y misión del SIS ECU-911, se considera que dicha entidad no sea contemplada como parte del subsistema de ciberseguridad ciudadana, sino como una entidad auxiliar que aporta, en el caso de considerarlo pertinente, con instrumentos para sistema nacional de seguridad, tales como un catálogo de incidentes o alertas hacia otras entidades competentes en la investigación de presuntos cometimientos de ciberdelitos. El SIS ECU-911, al recibir alertas sobre emergencias e incidentes mediante llamadas, videovigilancia o su aplicación, coordina la atención de las mismas con instituciones articuladas a ella, mismas que no tienen competencia alguna en la investigación de esta clase de delitos, sino únicamente de delitos clasificados como comunes; uso indebido y tráfico ilícito de sustancias estupefacientes y sicotrópicas, precursores químicos, enriquecimiento ilícito y testaferrismo en el país. Cabe recalcar que el SIS ECU-911 tiene convenios vigentes para la cooperación con la Función Judicial y sus órganos autónomos y jurisdiccionales, y la Agencia Nacional de Tránsito, mediante el intercambio de información captada en los sistemas de video vigilancia, audio y datos del SIS ECU-911, a fin de que sea analizada y evaluada dentro de un debido proceso judicial. El SIS ECU-911 no interviene en el proceso de investigación.

Remitente Fecha documento	Síntesis de observaciones
	2) En caso de mantener al SIS ECU-911, dentro de este subsistema, se sugiere cambiar el artículo por el siguiente texto: El subsistema de ciberseguridad ciudadana 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 Servicio Integrado de Seguridad ECU-911 y otras entidades que se consideren necesarias para resguardar la seguridad ciudadana y protección interna en el ciberespacio. • En el artículo 60, a fin de mantener la secuencia activa del control de los recursos y activos de la información, debería orientarse a la necesidad de la creación de un área específica de seguridad digital y así permita tener un control continuo de estas responsabilidades, en virtud de evitar la alta rotación de funcionarios NJS.
Efrén Guerrero, profesor de la facultad de jurisprudencia. PUCE S/O, de 24 de enero de 2024	Presenta observaciones a 12 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • El artículo 2 de la norma establece que se establecerá esta ley orgánica para poder hacer frente a amenazas e infraestructuras de seguridad cibernética. Considero que debe hacerse un alcance mucho más amplio a través de la norma para que pueda tener un efecto más claro y establecer como disposiciones transitorias cuáles son los reglamentos e instituciones que deben construirse mediante un plazo claro. • En el artículo 3, considero que en el artículo 3 numeral cuatro, se deben separar los elementos de inteligencia y ciberdiplomacia. El primero debe ser construido a través de una norma específica, dado que la recopilación, procesamiento y toma de decisiones a través de información estratégica debería tener una norma propia que pueda articular los diferentes sistemas de inteligencia en Ecuador, que se encuentran dispersos entre diferentes cuerpos y fuerzas de seguridad del Estado y con poca conexión con el brazo civil. Mientras tanto, el concepto de ciberdiplomacia debe ser construido mediante las actividades y la política que decida el Ministerio de Relaciones Exteriores, sin que sea una obligación legal, sino de la política exterior enmarcada en el artículo 416 de la CRE. • No hay una conexión entre el artículo 3, numeral 7, y el resto del proyecto de ley, dado que la cooperación internacional no depende de la promoción a través de la ley, sino de la existencia de una dinámica interna del sistema de cooperación internacional. • Creo que no debería establecerse la definición de ciberdelito o ciberdelincuencia dentro de esta norma, ya que esa es materia exclusiva del Código Orgánico Integral

Remitente Fecha documento	Síntesis de observaciones
	Penal. Una de las necesidades que debemos abordar en el país es la unificación de normas relativas al sistema punitivo solo en un código. La dispersión normativa genera problemas de inseguridad jurídica y afecta tanto la aplicación normativa como el ejercicio del derecho. • El artículo 6, que implica una serie de actividades protegidas, debería entenderse cuál es la consecuencia jurídica de la existencia de esas actividades. • En el artículo 7, debería hacerse una definición de cuáles son las infraestructuras críticas y estratégicas del sector público y privado en materia digital, puesto que en el artículo 6 se indica la categoría de "servicios esenciales", que puede ser confundida con servicios públicos, especialmente si gran parte de la legislación internacional y de la doctrina sobre derechos digitales asume que internet también debe ser entendido como un servicio público. • Los artículos del 13 al 15 proponen una serie de enfoques. Es importante tener en cuenta que no es lenguaje constitucional. Creo que deben construirse en la forma de principios para que sean consistentes con el artículo 11 de la Constitución y puedan aplicarse en el momento de la interpretación de esta ley por parte de una autoridad administrativa o judicial. Especialmente en el artículo 17, creo que es una repetición innecesaria de principios que ya pueden estar contemplados en el régimen de desarrollo constitucional. • Nuevamente se incluyen los artículos 19 a 21 como enfoques, cuando deben entenderse como principios. • En el artículo 22, debería incluirse dentro de la gestión de incidentes la judicialización obligatoria de estos incidentes y quién se encuentra responsable. Debería además establecerse quién debe ser el encargado de judicializar aquellos incidentes. • En el artículo 27, dada la rotación de ministerios o de entidades del ejecutivo, y dada la capacidad de crear esas instituciones a través del artículo 147 y 141 de la constitución, se propone no utilizar la expresión ministerio, sino ente rector. • La integración del sistema nacional de seguridad digital prevista en el artículo 27 debe tener otro tipo de organización. Tener más de 20 instituciones en un órgano colegiado puede generar una tremenda incapacidad para la toma de decisiones estratégicas en un tiempo corto, considerando la variedad y capacidad destructiva de las amenazas digitales. Considero que puede utilizarse como una buena práctica las propuestas realizadas en la Ley Orgánica Contra la Trata de Personas y Tráfico Ilícito de Migrantes, en la cual existe un comité interinstitucional con un número corto de organismos y

Remitente Fecha documento	Síntesis de observaciones
	una serie de mesas técnicas reunidas por sus capacidades y áreas de gestión de política pública, articuladas posteriormente mediante un reglamento. • El artículo 29 es importante, pero hay obligaciones que no son de un órgano colegiado, como, por ejemplo, la prevista en el numeral 6 respecto a "promover la confianza en el entorno digital". Eso es una política pública que debe hacerse por un ministerio. • El sistema, a su vez, no debe presentar informes (numeral 8), ya que es un organismo de nivel superior que solo debe tomar decisiones. La presentación de informes debe hacerse a través de los ministerios de línea. El numeral 9 queda muy abierto, dado que, si la ley orgánica construye un organismo con capacidades de toma de decisión a través de todos los ministerios, no se entendería quién debería generar las normas técnicas, y no es el mismo comité. • En el numeral 12, a su vez, se indica que el sistema va a notificar a las entidades con sus correspondientes los incidentes y ataques. Dada la velocidad y necesidad de medidas tanto de protección como contramedidas tecnológicas y electrónicas para evitar el aumento del daño, tanto en la infraestructura como en la información, considero que debe establecerse un solo organismo dentro de todos aquellos que son parte del comité y que debería estar encargado de la respuesta directa y la notificación a la institución para que active sus propios sistemas de protección de la información. • Me parece muy positivo que en el artículo 31 se establezca la obligación de un registro de dispositivos electrónicos en el ámbito público y privado. Creo que debe establecerse de manera urgente una obligación dentro de la ley que haga ese registro y, por otro lado, se le dé la oportunidad a través del mismo artículo de la cancelación automática de líneas o de acceso al sistema de los dispositivos que no realicen el registro. • Considero que debe hacerse una diferenciación clara de las competencias entre el comité y el sistema nacional de seguridad digital. Pareciera que el sistema es un cúmulo de organizaciones con muy poca capacidad de operación, mientras que el comité es un espacio más bien operativo. Con el objetivo de mantener regularidad administrativa y cumplir las obligaciones del Código Orgánico Administrativo. • Considero que el artículo 44 debe entenderse en el marco de las obligaciones de cooperación entre la Policía Nacional y las Fuerzas Armadas, ya que son fuerzas y cuerpos de seguridad del Estado. • El artículo 60, respecto al responsable de seguridad digital, considero que debe redactarse de forma que se

Remitente Fecha documento	Síntesis de observaciones
	entienda que el funcionario debe tener una formación tanto en seguridad digital como en manejo de tecnologías de la información y comunicación. Dado que son funcionarios operativos que deben generar estrategias de seguridad digital, deben tener una formación muy particular y deben ser funcionarios que puedan tener estabilidad independientemente del funcionario jerárquico superior. • En el artículo 69, debería incluirse como un instrumento para la respuesta frente a riesgos digitales y como un numeral aparte una norma técnica para la ejecución de mecanismos digitales dentro de los estados de excepción, dado que las amenazas antropogénicas obligan a contar con mecanismos previos para enfrentar a las emergencias.
Fabián Iñiguez Matute, Grupo Radical OFICIO-RDCAL-2024-01-009, de 24 de enero 2024	Presenta observaciones a 10 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 5, adicionar lo que es un equipo de respuesta a incidentes de seguridad informática o CSIRT: Equipos multidisciplinarios de expertos que tiene por objetivo prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas basados en mejores prácticas nacionales e internacionales. • En el artículo 29, se recomienda incluir un numeral que se refiera a la necesidad de contar con una seguridad digital proactiva por medio de monitoreo preventivo que permitirá identificar oportunamente las posibles vulnerabilidades de ciberseguridad. Esto es posible mediante la adopción de un centro de operaciones de ciberseguridad debidamente certificado: 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: (...). 18. Monitorear, detectar y notificación de alertas de ciberseguridad en un esquema 24x7 de manera proactiva a sus activos críticos digitales, por medio de un Centro de Operaciones de Ciberseguridad. Cabe señalar que los Centros de Operaciones de Ciberseguridad deben contar como mínimo con 4 certificaciones afines reconocidas a nivel internacional (...). • En el artículo 31, es necesario incluir este texto, toda vez que se recomienda que las auditorías sean realizadas por profesionales debidamente calificados y que cuenten con una certificación internacional en ciberseguridad. Artículo 31. Atribuciones del ente rector del Sistema Nacional de Seguridad Digital. E (...) (..) 8. Reglamentar la realización de auditorías para la seguridad de la

Remitente Fecha documento	Síntesis de observaciones
	información en el ámbito público y privado por medio de profesionales especializados en ciberseguridad con al menos una certificación internacional. • En el artículo 33, se encuentra repetido el siguiente texto: La máxima autoridad, la Secretaria General de la Administración Pública o su delegado permanente. Por lo que se sugiere eliminar el numeral 3 de dicho artículo. • En el artículo 39, se debe crear un equipo de respuesta a incidentes. El Centro de Respuesta a Incidentes de Seguridad Digital se debe crear en esta ley para dar la importancia a nivel internacional y asentar lo ya establecido en la Ley Orgánica de Transformación Digital. Artículo 39. Equipo Nacional 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. Crear dentro del ente rector en seguridad digital o Agencia Nacional de Seguridad Digital el Equipo Nacional de Respuesta a Incidentes de Seguridad digital, en adelante Ecucert y la Agencia de Regulación y Control de las Telecomunicaciones, debe renombrar su Centro de Respuesta a Incidentes de Ciberseguridad como CERT de Telecomunicaciones. 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. Los centros de respuesta a incidentes de ciberseguridad privados deben fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad. • En el artículo 50 numeral 5, dar directrices y evaluar asume funciones del ente rector, cambiar por asesorar. 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; porque se duplicaría con funciones que deben ejecutar las instituciones 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 ciberespacio; (eliminar porque se estaría tomando atribuciones del CERT nacional). • En el artículo 56, se debe realizar una seguridad digital

Remitente Fecha documento	Síntesis de observaciones
	proactiva por medio de monitoreo preventivo que permitirá identificar oportunamente las posibles vulnerabilidades de ciberseguridad con todas las entidades a su cargo y poder interactuar con el centro de respuesta a incidentes de seguridad digital, por lo que se requiere modificar el numeral 12 de dicho artículo por el siguiente; 12. Monitorear, detectar y notificación de alertas de ciberseguridad en un esquema 24x7 de manera proactiva a los activos digitales de las entidades a su cargo, los centros de operaciones de ciberseguridad deben contar como mínimo con 4 certificaciones afines reconocidas a nivel internacional. • En el artículo 58, se debe realizar un enfoque colaborativo y proactivo en la gestión de ciberseguridad del sector financiero ecuatoriano por medio de monitoreo preventivo y respuesta ante incidentes informáticos que permitirá identificar oportunamente las posibles vulnerabilidades de ciberseguridad con todas las entidades a su cargo y poder interactuar con el centro de respuesta a incidentes 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: (...). Texto propuesto: En el plazo de 90 días, a partir de la publicación en el Registro oficial, la Superintendencia de Bancos y la Superintendencia de Economía Popular y Solidaria deberán crear la normativa para que sus entidades supeditadas cuenten con un equipo de respuestas a incidentes debidamente certificado internacionalmente para fortalecer el esquema de identificación, prevención y gestión de incidentes digitales. • En el artículo 68, se recomienda que sea la agencia o el ente rector de la seguridad digital; por lo que, se sugiere modificar el artículo en el siguiente sentido: Artículo 68. Acreditaciones a operadores, proveedores y sistemas de información y comunicaciones. La Agencia o su equivalente acreditará. • En el artículo 74, se sugiere colocar en el segundo párrafo lo siguiente: (...). Las instituciones públicas y privadas deberán monitorear.
Diana Salazar Méndez, fiscal general del Estado Oficio No.FGE-DSP-2024-001378-O, de 19 de febrero de	Presenta observaciones a 9 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 5, en la definición de ciberdelito se recomienda cambiar la palabra culposa por "culpable", pues tiende a la confusión de que el ciberdelito se refiere a conductas imprudentes (culposas). • En el artículo 27, la Fiscalía General del Estado no puede pertenecer a un sistema nacional de seguridad digital

Remitente Fecha documento	Síntesis de observaciones
2024	cuyo destino es promover la seguridad digital. El ente acusador oficial del Estado solo se encarga de investigación preprocesal y procesal penal, así como la promoción de la acción penal pública, para cuyo caso cuenta con normativa suficiente y herramientas idóneas que le permite investigar ciberdelitos sin necesidad de formar parte de un sistema de seguridad digital. • En el artículo 29, ninguna función del sistema es concordante con las competencias constitucionales y legales que tiene la Fiscalía General del Estado, pudiendo incluso representar una merma en las investigaciones que lleva adelante la Fiscalía General del Estado en temas de ciberdelitos, el pertenecer al referido sistema. • En el artículo 33, de igual forma, incluir a la Fiscalía General del Estado como miembro del Comité Nacional de Seguridad Digital desdibuja y merma las funciones que esta institución debe cumplir en la investigación de delitos. • En el artículo 34, conforme se manifestó en el comentario general realizado al presente proyecto de ley, el numeral 1 del artículo 34 claramente determina que el comité nacional tendrá como atribución la generación de políticas públicas respecto a la seguridad digital, desconociendo que la Fiscalía General del Estado no genera dichas políticas y tampoco previene delitos, sino que persigue su comisión. Así mismo, todas las atribuciones restantes de este artículo no se corresponden, compaginan ni relacionan con ninguna atribución de la Fiscalía General del Estado. • En el artículo 45, el ente persecutor del Estado tampoco puede pertenecer a un subsistema de ciberseguridad ciudadana, pues conforme la normativa vigente, es la Fiscalía General del Estado la llamada a solicitar u obtener información necesaria a cualquier institución pública o privada para la investigación y judicialización de delitos cibernéticos, sin necesidad de estar anclada a un organismo colegiado en donde participan otras instituciones públicas que carecen de dichas competencias. Dicha propuesta incluso podría poner en riesgo la reserva de la información que la Fiscalía maneja en sus investigaciones y representaría una intromisión en la autonomía que este ente debe tener para cumplir su función constitucional. • En el artículo 47, se le está dando competencias al Ministerio del Interior que le corresponden exclusivamente a la Fiscalía General del Estado en el impulso de las investigaciones preprocesales y procesales penales de delitos de acción pública, específicamente en los numerales 3, 4, 5 y 11, pues el referido Ministerio no puede actuar como responsable de las investigaciones

Remitente Fecha documento	Síntesis de observaciones
	penales por ciberdelitos ni articular actividades en relación a las referidas investigaciones, mucho menos recopilar información dentro de las competencias del ente acusador oficial del Estado. • En el artículo 56, la Fiscalía General del Estado es un organismo autónomo de la Función Judicial, por ende, no necesita la vigilancia, intervención ni control en materia de seguridad digital por parte del Consejo de la Judicatura, pues incluso la institución titular de la acción penal pública cuenta y maneja su propio sistema interno al que no tiene acceso el Consejo de la Judicatura. En tal sentido, permitir que la referida institución pueda intervenir en temas de seguridad digital en la Fiscalía General del Estado merma su autonomía y pone en riesgo la información reservada y confidencial que se maneja en las investigaciones penales que se llevan a cabo. En consecuencia, se recomienda excluir de dichas facultades del Consejo de la Judicatura a la Fiscalía General del Estado. • En el artículo 57, conforme se ha establecido en la observación general, se recomienda que la Fiscalía General del Estado no sea incluida dentro del presente proyecto de ley como miembro del sistema, pues nuestras funciones constitucionales y legales las podemos cumplir en el ámbito de investigación de ciberdelitos sin necesidad de formar parte de organismos colegiados destinados a generar políticas públicas. De tal manera que se garantice la correcta institucionalidad de la Fiscalía General del Estado sin desdibujar su estructura, aparataje, funciones ni competencias. Además, no queda claro si la titular de la acción penal pertenece al sistema nacional de seguridad digital, al comité nacional de seguridad, al subsistema de seguridad ciudadana o funciona como un organismo auxiliar. De la misma manera, si observamos el numeral 3 del artículo 57, se evidencia que se le está otorgando la función de proponer políticas y estrategias de prevención a la FGE, apartándose de lo que la Constitución de la República determina en su artículo 195 en cuanto a la naturaleza y razón de ser de la Fiscalía General del Estado.
Magister Ralph Assaf, Servicio Ecuatoriano de Normalización INEN	Presenta observaciones a 9 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • Se sugiere para la redacción de los artículos 5, 7, 12, 22, 23, 24, 25 y 30, utilizar las mejores prácticas basadas en normas internacionales como por la familia de las normas ISO 27000. • En el artículo 59, los puntos 1, 2, 3, 6, 8, se deben eliminar en razón de que el contenido del artículo 59, no se ajusta a las competencias establecidas en la ley del sistema ecuatoriano de la calidad para el Servicio

Remitente Fecha documento	Síntesis de observaciones
	Ecuatoriano de Normalización-INEN. Se debe modificar el nombre de Instituto Ecuatoriano de Normalización a Servicio Ecuatoriano de Normalización, de conformidad a lo dispuesto en el Decreto Ejecutivo Nro. 338 del 16 de mayo de 2014, en la cual consta como Servicio Ecuatoriano de Normalización. Se recomienda modificar el texto del contenido de la siguiente manera: El Servicio Ecuatoriano de Normalización, en base a las atribuciones y funciones de su propia naturaleza, tendrá las siguientes: 1. Formular, en sus áreas de competencia, luego de los análisis técnicos respectivos, las propuestas de normas, reglamentos técnicos y procedimientos de evaluación de la conformidad, los planes de trabajo, así como las propuestas de las normas y procedimientos metrológicos. 2. 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; y, 3. Las demás establecidas en la Ley y su reglamento.
Jorge Guerrón, experto en ciberseguridad S/O, de 25 de enero de 2024	Presenta observaciones a 14 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 3, se sugiere ajustar el numeral 8. Fomentar una cultura de la ciberseguridad responsable en la ciudadanía, mediante el desarrollo de capacidades en ciberseguridad. • En el artículo 5, se sugiere eliminar la definición que debería estar en la Ley Orgánica de Telecomunicaciones: 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. • En el artículo 6, el experto sugiere: En el artículo 8 de la normativa se habla de activos de información, lo cual sería correcto al ser un concepto más amplio: b. Los activos de información de alto impacto; (...). • En el artículo 8, se sugiere eliminar lo que se encuentra en rojo: 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. • En el artículo 13, indica que, la seguridad digital se

Remitente Fecha documento	Síntesis de observaciones
	orientará por el plan nacional de seguridad integral, los planes específicos de defensa y seguridad pública y ciudadana, así como 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. • En el artículo 27, indica que, definir un mínimo de instituciones y designar las otras a los subsistemas: 1. El ente responsable de la coordinación de la seguridad pública y del Estado. 2. El rector del subsistema de ciberseguridad. 3. El rector del subsistema de ciberdefensas. 4. El rector del subsistema de ciberinteligencia. 6. El rector del subsistema de ciberdiplomacia. 7. El Comando Conjunto de Fuerzas Armadas. 8. Policía Nacional. • En el artículo 30, debería ser el ente responsable de la coordinación de la seguridad pública y del Estado o el Ministerio del Interior. • En el artículo 31, esta actividad operativa debería estar definida en la Ley Orgánica de Telecomunicaciones: 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. Actividades operativas que podrían ser asignadas al observatorio. 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. 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. Segregar actividades operativas a los subsistemas. Ciberinteligencia: 21. Emitir boletines y alertas de seguridad digital, seguridad sistémica y acceso a la verdad de los hechos; ciberseguridad: 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. • En el artículo 33, indica que, esta entidad no debería formar parte ya que es operativa: 9. La máxima autoridad de la Agencia de Regulación y Control de las Telecomunicaciones o su delegado permanente.

Remitente Fecha documento	Síntesis de observaciones
	• En el artículo 55, este artículo no debería formar parte del cuerpo legal y pasar a la LOT. Normativa específica operativa de la Ley Orgánica de Telecomunicaciones: 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. ¿Una entidad como la Arcotel, específica de las telecomunicaciones, podría sancionar a una de otro sector como la energía? 8. Ejercer el control, regulación y sanción a los proveedores de servicios esenciales y operadores nacionales de infraestructura estratégica y crítica digital. • En el artículo 60, indica que, el responsable de seguridad digital de las entidades públicas, 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. Adicionalmente agregar: Proveer información de amenazas y eventos de seguridad al rector del subsistema de ciberinteligencia. • En el artículo 61, se debe tener cuidado con mantener la siguiente normativa. La planeación institucional cambiará conforme se gestiona el riesgo y se mejoran los procesos institucionales. 5. Planes institucionales para la reducción, respuesta y recuperación ante riesgos, amenazas e incidentes digitales; ¿Se planea emitir una acreditación para la operación en el Ecuador de aplicaciones? 6. Acreditaciones a operadores, proveedores y sistemas de información y comunicaciones. Si se mantiene debe ser parte de la LOT, bajo el siguiente texto: 6. Acreditaciones a operadores y/o proveedores de sistemas de telecomunicaciones. • En el artículo 66, ¿cuál es el orden jerárquico? Plan nacional, plan sectorial/específico, estrategia. • En el artículo 68, tener cuidado de cómo se realizaría la acreditación, o eliminar.
Abogado Luis Enríquez, experto en ciberseguridad S/O, de 5 de febrero de 2024	Presenta observaciones a 10 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 3 numeral 2, cambiar amenazas por y perfilamiento de amenazas. • En el artículo 4, reemplazar en definición de autenticidad identificables por auténticos. Incluir definición de confidencialidad. Definición sugerida: Confidencialidad.

Remitente Fecha documento	Síntesis de observaciones
	Propiedad de que la información no será accesible ni compartida con personas naturales o jurídicas no autorizadas. (ISO / IEC 27000:2018). • En el artículo 5, tiene que incluirse una definición de riesgo, de gestión de riesgos y de análisis de riesgos. Riesgo. Una pérdida potencial, desastre u otro indeseable evento, medido con probabilidades asignadas a probables pérdidas de varias magnitudes. Gestión de riesgos. La identificación, análisis y priorización de riesgos que requieren de una coordinada implementación de recursos para reducir, monitorear, y controlar su probabilidad e impacto. Análisis de riesgos. La examinación detallada de los componentes de un riesgo, incluyendo la evaluación de varios eventos y de sus consecuencias, con el fin de tomar decisiones informadas. Hubbard (2020). • En el artículo 18, existen derechos digitales en la Ley de Protección de Datos Personales, no en la Constitución. Agregar en la Ley Orgánica de Protección de Datos Personales. • En el artículo 34, considerar que la seguridad de la información involucra también sistemas que no necesariamente están en red, como archivos. Agregar en numeral 1: (...) y otros entornos digitales. • En el artículo 37, agregar numeral 8. Establecer las directrices y procedimientos para la calificación de peritos en informática forense, fundamentado en las habilidades requeridas. Especialidad y experticia. • En el artículo 44, en el numeral 23. Las matrices de riesgo presentan varios problemas y ya no son un mecanismo de visualización de riesgo recomendado. Es mejor recomendar "distribuciones de probabilidades" (probability distributions), "curvas de exceso de pérdidas" (loss exceedance curves), y sobre todo recomendar una lógica de ciber valor al riesgo (Cy-VaR). • En el artículo 56, en el numeral 6, reemplazar texto por: Calificar a peritos en informática forense en base a los lineamiento y directrices establecidos por el Consejo Nacional de Seguridad. Considerar que el Consejo de la Judicatura no está preparado para esto y su personal no tiene los conocimientos necesarios en un área tan importante. Actualmente hay una sola persona que califica peritos, el sistema ahuyenta talentos, y se fundamenta en requisitos irrelevantes, sin considerar las competencias y habilidades prácticas necesarias. Debería reconsiderarse más bien que el consejo de seguridad establecido en esta ley, recomiende los peritos en informática forense, y el Consejo de la Judicatura acepte dichas recomendaciones. También considerar un régimen especial para los peritos en informática forense, pues las

Remitente Fecha documento	Síntesis de observaciones
	herramientas son costosas, mucho más que en otras áreas de peritaje. • En el artículo 60, en el numeral 3 reemplazar confiabilidad por confidencialidad. • En el artículo 76, reemplazar en numeral 1 "el posible daño en el caso de amenaza" por "el daño probable en caso de ocurrir el incidente".
Señor Gian Carlo Loffredo Rendón. Ministerio de Defensa Nacional Oficio Nro. MDN-MDN-2024-0114-OF, de 15 de enero de 2024 Oficio Nro. MDN-GAB-2024-163-TEMP, de 28 de febrero de 2024	Presenta observaciones a 58 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 1, se sugiere eliminar la frase u otros entornos digitales, debido a que en el objeto de la ley establece el ciberespacio y otros entornos digitales, sin embargo, se propone dejar únicamente ciberespacio, ya que, de acuerdo con la definición establecida para ciberespacio, esta abarca a otros entornos digitales (en el artículo 5 página 76). • En el artículo 2, se sugiere eliminar la frase u otros entornos digitales, debido a que en el objeto de la ley establece el ciberespacio y otros entornos digitales, sin embargo, se propone dejar únicamente ciberespacio, ya que, de acuerdo con la definición establecida para ciberespacio, esta abarca a otros entornos digitales. • En el artículo 3, se sugiere modificar el numeral 1 del artículo 3, infraestructuras críticas por infraestructuras críticas digitales, en razón de que las infraestructuras críticas no tienen una relación directa con el ciberespacio y tampoco dan a entender que se trata del ámbito digital, en tal virtud, se debería modificar por infraestructuras críticas digitales, ya que estas son las que se identifican y operan en el ciberespacio. • En el artículo 4, se sugiere eliminar del numeral 4 del artículo 3 la expresión determinar las características, ya que no es parte de la gestión de incidentes como lo establece en el artículo 22. Gestión de riesgos e incidentes en el ámbito digital. Del presente proyecto de ley, cuyo contenido ha sido complementado, como parte de esta propuesta. Así mismo, se recomienda incluir la palabra riesgos para tener concordancia con la estructura y articulados que se mencionan a lo largo del presente proyecto de ley. Se sugiere, incluir: el numeral 11, debido a que la defensa en y a través del ciberespacio, requiere el apoyo y colaboración obligatoria de todos los poderes del Estado, así como la alianza internacional para combatir amenazas y riesgos nacionales y transnacionales, que atenten a los intereses del Estado. • En el artículo 4, se sugiere modificar en el artículo 4 el principio de oportunidad debido a que todos los subsistemas, entre ellos el de ciberdefensa, actúa en las operaciones militares de forma oportuna, inmediata, lo que permite obtener un impacto efectivo a nivel local,

Remitente Fecha documento	Síntesis de observaciones
	regional o mundial, frente a ciberamenazas que se identifiquen. (Artículo 51 de la carta de las Naciones Unidas). Se sugiere incluir en el artículo 4 los tres principios, de legalidad, legitimidad y proporcionalidad, debido a que es el marco de aplicación para afrontar amenazas o crisis con el empleo de todos los poderes del Estado. En el caso del ámbito ciberespacial, se debe evitar efectos que podrían impactar a la seguridad nacional, además contribuir con estas acciones a la seguridad digital región o mundial. • En el artículo 6, se sugiere incluir la palabra digital, en el término infraestructura crítica debido a que, en las infraestructuras críticas existen la digital y la física, y esta ley está orientada a la seguridad digital. Y eliminar la palabra estratégica, debido a que la infraestructura estratégica incluye varias categorías y la presente ley está orientada al ámbito digital. • En el artículo 7, se sugiere incluir la palabra digital, en el término infraestructura crítica debido a que, en las infraestructuras críticas existen la digital y la física, y esta ley está orientada a la seguridad digital. Adicionalmente, se sugiere eliminar la palabra estratégica, debido a que la infraestructura estratégica incluye varias categorías y la presente ley está orientada al ámbito digital. • En el artículo 9, se sugiere modificar el artículo 9, la frase proveniente del ciberespacio u otros entornos por en y a través del ciberespacio, tal cual se propuso en la definición de ciberespacio, que consta en el artículo 5 de la presente propuesta. • En el artículo 22, se sugiere modificar los procesos principales del artículo 22, debido a que existen metodologías de gestión de riesgos como Magerit, ISO 27001 e ISO 31000, que consideran cinco procesos, y en el artículo antes referido, solo constan tres. • En el artículo 23, se sugiere modificar el título del epígrafe y el contenido del artículo 23, para guardar relación con lo expuesto en el artículo 22 propuesto, que remplaza los 3 procesos principales por 5, que establecen que se debe conocer todos los activos de información, para priorizar la criticidad, de acuerdo con las políticas y estrategias institucionales. Cabe señalar que, con el artículo 22 propuesto, se debe modificar la numeración del articulado a partir del artículo 24 propuesto. Se sugiere agregar un nuevo artículo que trate sobre la identificación y categorización de vulnerabilidades de los activos de información, para guardar relación con lo expuesto en el artículo 22 propuesto, que remplaza los 3 procesos principales por 5, en razón de que se hace necesario conocer cada proceso en la gestión de riesgos e

Remitente Fecha documento	Síntesis de observaciones
	incidentes en el ámbito digital. • Se debe eliminar el artículo 24, para guardar relación con lo expuesto en el artículo 22 propuesto, que remplaza los 3 procesos principales por 5, este artículo eliminado se encuentra modulado y fusionado con el artículo 25, por lo que pasará a ser descrito en el artículo 27 propuesto. Se sugiere incluir el artículo 25, para guardar relación con el artículo 22 propuesto en el presente proyecto de ley, que remplaza los 3 procesos principales por 5, debido a que una vez identificado los activos de información se debe identificar las amenazas relacionadas de acuerdo a metodologías como Magerit, ISO 27001 e ISO 31000. • Se debe eliminar el artículo 25, para guardar relación con lo expuesto en el artículo 22 propuesto, que remplaza los 3 procesos principales por 5, este artículo eliminado se encuentra modulado y fusionado con el artículo 24, por lo que pasará a ser descrito en el artículo 27 propuesto. Se sugiere incluir el artículo 26, para guardar relación con el artículo 22 propuesto en el presente proyecto de ley, que remplaza los 3 procesos principales por 5, debido a que existen metodologías que, para calcular el riesgo, establecen que se debe relacionar las amenazas con los activos de información de acuerdo con metodologías como Magerit, ISO 27001 e ISO 31000. • Se sugiere incluir el artículo 27, para guardar relación con el artículo 22 propuesto en el presente proyecto de ley, que remplaza los 3 procesos principales por 5, debido a que se modulan y fusionan los artículos 24 y 25. Considerando que, en la respuesta a riesgos e incidentes, se incluye la recuperación de acuerdo con metodologías como Magerit, ISO 27001 e ISO 31000. • Se sugiere incluir en el artículo 29 renumerado 31, como primer numeral, identificar y evaluar los activos de información de la institución o ámbito de su competencia, debido a que es necesario primero conocer sobre qué activos de información se está tratando, antes de identificar y evaluar vulnerabilidades. Luego de la inclusión del primer numeral, se mantiene lo que consta en el proyecto de ley. • En el artículo 30, propone, la rectoría del sistema nacional de seguridad digital será responsabilidad del organismo político estratégico, coordinador del sistema de seguridad pública y del Estado o quien haga de sus veces. • En el artículo 31, se sugiere, el rector del sistema nacional de seguridad digital será el organismo político estratégico, coordinador del sistema de seguridad pública y del Estado o quien haga de sus veces, tendrá las siguientes atribuciones y funciones. • En el artículo 33, se sugiere en el numeral 11 del artículo

Remitente Fecha documento	Síntesis de observaciones
	33 renumerado 35 se cambie la palabra "cibernética" por "digital", debido a que la ley trata de seguridad digital y no de seguridad cibernética, de igual manera es importante señalar que los términos digital y cibernético no son sinónimos, cada uno tiene su propia definición. • En el artículo 37, se recomienda modificar en el numeral 4 del artículo 37 renumerado 39, debiendo cambiar la palabra "en" por "el". • En el artículo 40, se recomienda modificar en el numeral 6 del artículo 40 renumerado 42, la palabra "cibervulnerabilidades" por "vulnerabilidades", debido a que no forma parte del objeto del presente proyecto de ley ni se encuentra definida cibervulnerabilidades en el artículo 5, definiciones. Sin embargo, el término vulnerabilidad se encuentra establecido en el artículo antes citado. • En el artículo 41, se recomienda modificar el artículo 41 renumerado 43, el término cibernéticos por informáticos, debido a que no forma parte del objeto del presente proyecto de ley ni se encuentra definido cibernéticos en el artículo 5, definiciones. • Se sugiere modificar el artículo 42 renumerado 44, el término "unidad" por "entidad", debido a que en Fuerzas Armadas la unidad puede ser un batallón, un escuadrón, mientras que el organismo que hoy es el comando de ciberdefensa se proyecta a ser fuerza ciberespacial, de acuerdo con la política nacional de ciberseguridad. En el inciso segundo del artículo 42 renumerado 44, se recomienda agregar el término mitigación, ya que amplía las funciones de los subsistemas, permitiendo agregar la posibilidad de gestionar la probabilidad de ocurrencia de un ciberataque y el impacto en caso de materializarse. • Se sugiere modular el numeral 7 del artículo 44 renumerado 46, para modificar el significado del término infraestructura crítica nacional por infraestructura crítica digital, considerando que la infraestructura crítica abarca la digital y la física, para efectos de esta ley y del ente rector del sector defensa, es la infraestructura crítica digital la que se debe atender. • Se recomienda modificar el numeral 8 del artículo 44 renumerado 46, debido a que el subsistema de ciberdefensa no solo evalúa las vulnerabilidades, sino que también identifica y analiza amenazas para calcular el riesgo, a fin de garantizar el efectivo control y vigilancia del ciberespacio a través de ciberoperaciones. • Se sugiere incluir en el numeral 9 del artículo 44 renumerado 46 dentro de requerimientos de personal, equipamiento, datos y presupuesto, debido a que es importante especificar los tipos de requerimientos, a fin de no dar lugar a una generalidad y sean atendidos

Remitente Fecha documento	Síntesis de observaciones
	conforme la necesidad presentada. • Se recomienda cambiar en el numeral 10 del artículo 44 renumerado 46, la palabra "monitoreo" por "control", debido a que el seguimiento y monitoreo son sinónimos, requiriendo incluir al control de las vulnerabilidades, amenazas, incidentes y riesgos. • Se recomienda modificar el numeral 12 del artículo 44 renumerado 46, debido a que para poder responder ante amenazas en el ciberespacio es necesario iniciar actividades previas como la de recopilar indicios, reportando oportunamente al Comité Nacional de Seguridad Digital, para una adecuada toma de decisiones. • Se sugiere cambiar en el numeral 13 del artículo 44 renumerado 46 el término infraestructura informática por infraestructura crítica digital, debido a que no forma parte del objeto del presente proyecto de ley ni se encuentra definida infraestructura informática en el artículo 5, definiciones. • Se recomienda unificar los numerales 15 y 17 por similitud de contenido. • Se recomienda eliminar el numeral 16 del artículo 44, debido a que no se especifica qué registro evaluaciones se debe presentar. • Se debe eliminar el numeral 17 del artículo 44, debido a que se unificó con el numeral 15 por repetición. • Se recomienda modular el numeral 20 renumerado 18 del artículo 44 renumerado 46, eliminando las palabras tanto y táctica y operativa, debido a que son niveles que se deben especificar en el reglamento para el cumplimiento de la ley. • Se recomienda modificar el numeral 21 renumerado 19 del artículo 44 renumerado 46, de acuerdo con el modelo educativo de FF.AA., en el que se establecen los procesos para el desarrollo de talento humano en el área de su especialidad. • Se recomienda eliminar el numeral 24 renumerado 22 del artículo 44 renumerado 46, las palabras operativas y tácticos y estratégica, debido a que la forma cómo se recolecte la información debe constar en el reglamento de aplicabilidad. • Se recomienda eliminar el numeral 26 del artículo 44 renumerado 46, debido a que el proceso de formación fue establecido en el numeral 19 propuesto en el artículo 46 propuesto. • Se recomienda eliminar en el epígrafe y en el artículo 78 renumerado 80, el término seguridad sistémica y cambiar la palabra cibernética por digital, debido a que no forma parte del objeto del presente proyecto de ley, ni se encuentra definidos en el artículo 5, definiciones.

Remitente Fecha documento	Síntesis de observaciones
	• Se sugiere agregar un capítulo que trate del régimen sancionatorio, a fin de que el ente rector sancione las acciones u omisiones para las personas naturales, jurídicas, públicas, privadas, nacionales o extranjeras que incumplieren sus obligaciones o contravinieren las disposiciones de la Ley Orgánica de Seguridad Digital, siempre que estas inconductas no constituyan delitos y se encuentren tipificados en el Código Orgánico Integral Penal. Capítulo VII. Régimen sancionatorio. Artículo XXX. Responsabilidad administrativa. Las personas naturales, jurídicas, públicas, privadas, nacionales o extranjeras que por acción u omisión incumplan las disposiciones y obligaciones constantes en la presente ley, la normativa que emita el ente rector y demás que sean aplicables, incurrirán en responsabilidades administrativas que será sancionadas en ejercicio de la competencia y jurisdicción que se le concede al ente rector del sistema de seguridad digital, siempre que referidas acciones u omisiones, no constituyan delitos. Las sanciones administrativas se aplicarán conforme a lo que determine el reglamento general a la presente ley y se aplicarán, conforme a las garantías básicas de derecho a la defensa y del debido proceso. Para efectos de la aplicación de las mismas, las faltas se clasificarán en: leves, graves y muy graves.
Doctora Mónica Rosa Irene Palencia Núñez, ministra de Gobierno Oficio Nro. MDG-MDG-2024-0035-O, de 09 de enero de 2024	Presenta observaciones a 3 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • Se Incorporar soberanía digital como principio, en el artículo 4 de la Ley Orgánica de Seguridad Digital. • En el capítulo III, subsistemas del sistema nacional de seguridad digital de la Ley Orgánica de Seguridad Digital, se propone: la creación de un órgano centralizado con competencia exclusiva en ciberdefensa, dotándolo de la autoridad necesaria para coordinar y ejecutar acciones destinadas a salvaguardar la seguridad digital. Este ente será responsable de planificar, implementar y supervisar estrategias integrales de ciberseguridad, asegurando la protección de la infraestructura crítica y la información sensible. • Incorporar como disposición general el compromiso de análisis de adhesión a tratados internacionales en ciberseguridad, considerando que, a la fecha, Ecuador no es signatario del Convenio de Budapest sobre ciberdelincuencia; se establece el compromiso de evaluar y, en su caso, promover la adhesión de Ecuador a tratados internacionales relevantes en materia de ciberseguridad. Con el propósito de agilizar este proceso, se dispone a la Comisión de Relaciones Internacionales tramitar como prioritario cualquier gestión relacionada con la adhesión a dicho tratado.

Acta 922-A

Remitente Fecha documento	Síntesis de observaciones
Doctora Mónica Rosa Irene Palencia Núñez, ministra del Interior (E) Oficio Nro. MDI-DMI-2024-0474-OF, 18 de febrero de 2024	Presenta observaciones a 60 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 1, 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 y ciberinteligencia; 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. • En el artículo 2, las disposiciones de la presente ley son de cumplimiento obligatorio para todas las personas naturales o jurídicas que utilicen el internet para la transferencia de información o datos desde o hacia el Ecuador. • En el artículo 3, en el numeral 1, fortalecer y proteger en entornos digitales, infraestructuras críticas y servicios esenciales públicos y privados y fomentar la resiliencia de los sistemas de información. En el numeral 4. Establecer procedimientos para identificar, determinar las características y gestionar los incidentes cibernéticos a nivel nacional de manera sistémica. • En el artículo 4, se sugiere: La aplicación de la presente ley se rige por los principios previstos en la Constitución de la República, para la protección de los ciudadanos y ciudadanas, los instrumentos internacionales vigentes en Ecuador y los siguientes: (...). • En el artículo 5, se observarán las siguientes definiciones: Auditoría de ciberseguridad. Es el estudio periódico de cumplimiento para determinar la garantía de ciberseguridad, así como las evaluaciones de riesgos, pruebas de penetración y revisión de controles de seguridad, además de medir el cumplimiento de las políticas. Este proceso se aplica a los sujetos, redes, infraestructuras y sistemas que determine la presente ley. Amenaza. Es cualquier acción dirigida a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de este, con la intención de vulnerar una red, sistema o infraestructura con propósitos contrarios a la ley. Estas amenazas pueden originarse desde diversas fuentes, como actores estatales, ciberdelincuentes, ciberactivistas, ciberterroristas, competidores comerciales y otros. Ataque. Abarca actividades maliciosas que comprometen la disponibilidad, confiabilidad, integridad y confidencialidad de la información. Esto incluye el acceso no autorizado, la modificación, la degradación, pérdida de información, o la destrucción de sistemas de información y telecomunicaciones. Es una definición

Remitente Fecha documento	Síntesis de observaciones
	amplia que abarca varios tipos de ataques cibernéticos. Ciberespionaje. Actividades originadas o patrocinadas por diversas entidades con la intención de apropiarse de información sensible que afecte la seguridad del Estado, de las organizaciones o de las personas. Es importante destacar que el ciberespionaje puede tener objetivos políticos, militares, económicos o de otro tipo. Entornos digitales. Cualquier espacio, plataforma, red o sistema digital que no esté explícitamente definido como ciberespacio, pero que sea susceptible de ser afectado por amenazas, riesgos e incidentes relacionados con la seguridad digital. Esto puede incluir, entre otros, sistemas de información internos de organizaciones, aplicaciones móviles, entornos de computación en la nube, dispositivos IOT (Internet de las cosas), y cualquier otro entorno digital que pueda ser objeto de acciones maliciosas o representar riesgos para la seguridad digital y la protección de datos. 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. Seguridad digital. La seguridad digital se refiere a la protección de datos, información y sistemas en el entorno digital contra accesos no autorizados, pérdida, alteración o robo. Incluye medidas como firewalls, software antivirus, cifrado de datos y políticas de acceso para prevenir ataques cibernéticos y otras amenazas digitales. Seguridad sistémica. La seguridad sistémica aborda la protección y la gestión de sistemas complejos en general, considerando la interacción entre diferentes componentes y las posibles vulnerabilidades y riesgos. Se preocupa por comprender y mitigar los riesgos dentro de sistemas más grandes, tanto en el ámbito tecnológico como en otros aspectos de la sociedad, y se enfoca en la resiliencia y la capacidad de recuperación ante eventos disruptivos o ataques. • En el artículo 6, se sugiere lo siguiente: La presente ley protege: a. La infraestructura crítica, estratégica y los servicios esenciales. b. Los sistemas de información. c. La seguridad y defensa en el ciberespacio. d. Los derechos fundamentales en el ámbito digital, conforme a los establecidos en la Constitución y el ordenamiento jurídico nacional. e. Las comunicaciones digitales. f. La promoción de la cultura de ciberseguridad y la alfabetización digital. • En el artículo 9, se sugiere: se protege y defiende los activos de información, infraestructura, servicios y actividades cuya afectación puede amenazar la seguridad

Remitente Fecha documento	Síntesis de observaciones
	y (...). • En el artículo 10, se sugiere: se protege los derechos en general y en particular la integridad, confidencialidad y disponibilidad de los datos de las personas frente a los riesgos asociados con los delitos informáticos. • En el artículo 11, se sugiere: eliminar porque se requieren hacer inversiones a nivel de Gobierno, del Estado y de las instituciones para poder generar estándares, protocolos y reglas de comunicación y de utilización de los sistemas digitales que permitan articularse con otros países de la región y del mundo. • En el artículo 13, se sugiere: la seguridad digital se orientará por la estrategia nacional de seguridad digital que reflejará la visión del Estado y de la sociedad ecuatoriana respecto de los objetivos en materia de protección de la soberanía, seguridad integral, infraestructuras críticas y servicios esenciales públicos y privados, así como el fomento de la resiliencia de los sistemas de información en el entorno digital. • En el artículo 14, se sugiere: la seguridad digital fomentará la confianza en el entorno digital y promoverá la innovación y la adopción de tecnologías digitales de manera segura y responsable. • En el artículo 15, se sugiere: la seguridad digital desde un enfoque sistémico considerará todos los elementos interconectados y las interacciones dentro de un sistema complejo de información y tecnología. • En el artículo 16, se sugiere: la seguridad digital desde un enfoque multisectorial y multidimensional reconocerá que la protección de los sistemas digitales y la información no es responsabilidad exclusiva de un solo sector o área de la sociedad, sino que requiere la colaboración y el compromiso de múltiples actores en diferentes niveles. • En el artículo 17, se sugiere: la seguridad digital desde un enfoque de desarrollo sostenible implica integrar consideraciones de seguridad digital en las estrategias y acciones que promueven un desarrollo equitativo, inclusivo y sostenible en la era digital. • En el artículo 18, se sugiere: en la aplicación de la ley y el desarrollo de las políticas públicas se garantizará el ejercicio de los derechos digitales, conforme lo establecido en los instrumentos internacionales de derechos humanos suscritos por el Ecuador. • En el artículo 19, se sugiere: las políticas, planes, programas, proyectos y acciones (...), enfaticen prevención, actualización rápida y eficaz ante un incidente informático que permita tomar las medidas de recuperación, (...). • En el artículo 20, se sugiere: para promover la seguridad

Remitente Fecha documento	Síntesis de observaciones
	digital, es esencial que todos los actores del sistema, incluyendo la sociedad civil, las empresas privadas, las personas naturales nacionales o extranjeras, así como las entidades gubernamentales a nivel central y descentralizado, articulen esfuerzos, colaboren y ejecuten (...). • En el artículo 21, se sugiere: la seguridad digital tiene como objetivo fundamental promover la confianza en el entorno digital. Esto se logrará mediante la garantía de la seguridad de la información de los activos digitales, aprovechando las oportunidades que ofrecen las tecnologías de la información y comunicación, así como las tecnologías emergentes para el desarrollo del entorno digital. El fomento de la confianza digital será una prioridad en todas las acciones y políticas relacionadas con la seguridad digital. • En el artículo 22, se sugiere: gestión de incidentes: La gestión de incidentes en el contexto digital implica detectar, responder y recuperarse de incidentes de seguridad de manera efectiva y eficiente. Los procesos incluyen: 1. Implementar sistemas y herramientas de monitoreo para detectar actividades sospechosas o anomalías en la red y los sistemas digitales. 2. Clasificar y priorizar los incidentes detectados según su gravedad y su impacto potencial en la organización. 3. Investigar y analizar los incidentes detectados para comprender su naturaleza y alcance, y tomar medidas inmediatas para contener y mitigar el impacto. Notificar a las partes interesadas relevantes, incluidos el equipo de respuesta a incidentes, la dirección de la organización y las autoridades pertinentes, según sea necesario. 4. Realizar una investigación exhaustiva de los incidentes para determinar su causa raíz, recopilar evidencia digital y apoyar los esfuerzos de respuesta y recuperación. 5. Restaurar los sistemas y datos afectados por el incidente, implementar medidas correctivas para prevenir futuros incidentes similares y llevar a cabo actividades de seguimiento y revisión para evaluar la eficacia de la respuesta. • Las instituciones 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, y las vulnerabilidades, amenazas y riesgos de las tecnologías de información y comunicación. • En el artículo 25, se sugiere: el proceso de recuperación integra los subprocesos y componentes que permiten la restauración de los activos de información al Estado previo al incidente y mantener la continuidad mediante la redundancia; (...).

Remitente Fecha documento	Síntesis de observaciones
	• En el artículo 26, se sugiere: el sistema nacional de seguridad digital es una estructura integral que facilita la colaboración entre instituciones gubernamentales, entidades del sector privado y la sociedad civil para desarrollar políticas, normativas y estrategias que protejan la infraestructura digital y los datos sensibles, gestionen los riesgos cibernéticos mediante la identificación y evaluación de amenazas, implementen medidas de prevención y respuesta a incidentes, y promuevan la capacitación y concientización en seguridad digital entre todos los actores relevantes. • Se sugiere eliminar el artículo 27. • Se sugiere eliminar el artículo 29. • En el artículo 30, se sugiere: la rectoría del sistema de seguridad digital la tendrá la entidad rectora de la seguridad ciudadana, protección interna y orden público. • En el artículo 32, se sugiere: el comité nacional seguridad cibernética (...). • En el artículo 33, se sugiere: el comité nacional de seguridad cibernética, estará integrado por: 1. La máxima autoridad del ente rector del sistema de seguridad digital, quien lo presidirá y contará con voto dirimente. 2. La máxima autoridad del ente rector de la defensa nacional. 3. La máxima autoridad del ente rector de telecomunicaciones y sociedad de la información; (...). 6. La máxima autoridad de la Superintendencia de Protección de Datos; (...). • En el artículo 34, se sugiere: serán atribuciones del Comité Nacional de Seguridad Cibernética las siguientes: 1. Desarrollar políticas y estrategias para proteger los activos digitales y mitigar los riesgos cibernéticos. 2. Analizar y evaluar riesgos cibernéticos para identificar amenazas y vulnerabilidades. 3. Implementar medidas y controles de seguridad cibernética para mitigar los riesgos identificados. 4. Coordinar la respuesta a incidentes cibernéticos, incluida la detección, notificación, contención y recuperación. 5. Promover la capacitación y concientización en seguridad cibernética entre empleados y partes interesadas. • En el artículo 35, se sugiere: el Comité Nacional de Seguridad Cibernética 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 (...). • En el artículo 36, se sugiere: El secretario del Comité Nacional de Seguridad Cibernética será designado de

Remitente Fecha documento	Síntesis de observaciones
	entre las o los servidores de la entidad rectora de la seguridad digital y durará en el cargo por un periodo de dos años, renovable por una sola vez. • En el artículo 37, sugiere mejorar la redacción. Las atribuciones del secretario del comité nacional de seguridad cibernética, además de las establecidas por ley, incluyen: (...) 2. Elaborar las actas de las sesiones y suscribirlas conjuntamente con la presidenta o presidente del comité. 3. Mantener el registro de actas y el archivo físico o digital de la documentación del comité, asegurando la preservación histórica de la institución, incluyendo los convenios de cooperación nacionales e internacionales, los cuales estarán disponibles para las instituciones del sistema, conforme al reglamento de esta ley. 4. Servir como enlace entre las diferentes entidades que conforman el comité. 5. Certificar las actuaciones y los documentos emanados del comité. 6. Preparar respuestas a las solicitudes de información sobre resoluciones y actividades del comité. 7. Facilitar el acceso del público a la información no clasificada sobre el trabajo del comité, mediante los medios tecnológicos designados para tal fin. 8. Realizar seguimiento de los acuerdos y resoluciones adoptados por el comité. 9. Cumplir con las demás atribuciones establecidas en el reglamento general de aplicación de esta ley y en la normativa para el funcionamiento del comité. • En el artículo 38, se sugiere considerar la eliminación del artículo que propone la coordinación del sistema de seguridad pública y del Estado con el sistema nacional de seguridad digital. • En el artículo 42, se sugiere: el subsistema de ciberdefensa estará integrado por el ministerio rector de la defensa nacional y la unidad respectiva del Comando Conjunto de las Fuerzas Armadas. Este subsistema mantendrá una estrecha coordinación y colaboración con los subsistemas de ciberseguridad y ciberinteligencia. Estas colaboraciones permitirán el intercambio de información crucial para la adecuada defensa, prevención, respuesta y recuperación ante riesgos, amenazas e incidentes en el ciberespacio que puedan comprometer la soberanía del Estado. • En el artículo 41 se sugiere que la 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 Nacional de Seguridad Digital que será asumido y presidido por el ente rector de Seguridad Ciudadana, protección interna y orden público, quien gozará de voto

Remitente Fecha documento	Síntesis de observaciones
	dirimente; o su delegado permanente; (...). • En el artículo 51, se sugiere eliminar. • En el artículo 53, se sugiere eliminar. • En el artículo 55, se sugiere incluir el numeral 8. 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. • Se sugiere eliminar el artículo 56. • En el artículo 66, se sugiere el siguiente texto: 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 adecuados y medibles para evaluar la efectividad de las acciones implementadas. • En los artículos 74 al 76, se sugiere eliminar la recomendación por parte de ciberdelitos por abordar desde un enfoque diferente. • En el artículo 78, se sugiere cambiar la palabra cibernética por digital. • Se sugiere incluir un nuevo artículo referente al fondo para la seguridad digital sistémica. Se establece la creación de un fondo para la seguridad digital sistémica, con el propósito de garantizar la protección y fortalecimiento de los subsistemas digitales en el ámbito nacional. Este fondo estará destinado a financiar proyectos, investigaciones y medidas destinadas a mejorar la seguridad digital sistémica y prevenir amenazas sistémicas en el ciberespacio. El fondo para la seguridad digital sistémica será administrado por la entidad rectora del sistema nacional de seguridad digital, la cual estará encargada de gestionar los recursos de manera eficiente y transparente, en línea con los objetivos establecidos por la presente ley. Los recursos del fondo podrán provenir de asignaciones presupuestarias, donaciones, cooperación internacional, así como de multas y sanciones impuestas por violaciones a la seguridad digital. Los criterios de asignación de recursos del fondo se determinarán con base en la evaluación de riesgos y necesidades en materia de seguridad digital, así como en la identificación de áreas prioritarias para la prevención y respuesta ante amenazas, riesgos e incidentes en el ciberespacio, conforme al reglamento general a la presente ley. El fondo para la seguridad digital sistémica financiará acciones como: 1. Desarrollo y actualización de infraestructuras de

Remitente Fecha documento	Síntesis de observaciones
	seguridad digital a nivel nacional. 2. Capacitación y formación de profesionales especializados en seguridad digital. 3. Investigación y desarrollo de tecnologías innovadoras para la protección de sistemas digitales. 4. Implementación de políticas y normativas que promuevan la seguridad digital. 5. Fortalecimiento de la cooperación nacional e internacional en materia de seguridad digital; y, 6. Las que definan en el reglamento de la presente ley. • Incluir un nuevo artículo referente a: Responsabilidad. Las personas naturales, jurídicas, públicas, privadas, nacionales o extranjeras que por acción u omisión incumplan las disposiciones y obligaciones constantes en la presente ley, la normativa que emita el ente rector del sistema nacional de seguridad digital y demás que sean aplicables, incurrirán en responsabilidades administrativas que será sancionadas en ejercicio de la competencia y jurisdicción que se le concede al indicado ente rector, siempre que referidas acciones u omisiones, no constituyan delitos. Las sanciones administrativas se aplicarán, conforme a lo que determine el reglamento general a la presente ley y se aplicarán y a las garantías básicas de derecho a la defensa y del debido proceso. Para efectos de la aplicación de las mismas, las faltas se clasificarán en: leves, graves y muy graves. El ente rector del sistema nacional de seguridad digital verificará la implementación de los protocolos, procesos y procedimientos en la entidades públicas y privadas que expida para ambos sectores. En caso de incumplimiento de los protocolos y procedimientos definidos, podrá adelantar un proceso administrativo sancionatorio de conformidad con la normativa vigente y lo dispuesto en la presente ley. • Incluir un nuevo artículo, referente a: De las faltas leves. Para efectos de la presente ley se consideran faltas leves, las siguientes acciones u omisiones cometidas por personas naturales o jurídicas, públicas o privadas, nacionales o extranjeras: a) Entregar fuera de plazo, injustificadamente, la información que se le requiera cuando ella no fuere necesaria para la gestión de una amenaza, riesgo o incidente en el ciberespacio. b) Incumplir las instrucciones generales o particulares impartidas por el ente rector del sistema nacional de seguridad digital en los casos que no esté sancionado como infracción grave o gravísima. c) No mantener el registro de las acciones de seguridad adoptadas. d) No contar con programas de capacitación, formación y educación continua para los servidores y trabajadores

Remitente Fecha documento	Síntesis de observaciones
	sobre seguridad digital. e) No comunicar según se establece en el reglamento al ente rector del sistema nacional de seguridad digital la realización continua de operaciones de revisión, ejercicios y demás acciones que se ejecuten dentro del ámbito de sus competencias en materia de seguridad digital, de conformidad con los plazos correspondientes; y, f) Cualquier incumplimiento a las obligaciones que esta ley establece y que no tenga señalada una sanción especial. • Incluir un nuevo artículo sobre: De las faltas graves. Para efectos de la presente ley se consideran faltas graves las siguientes acciones u omisiones cometidas por personas naturales o jurídicas, públicas o privadas, nacionales o extranjeras: a) No haber implementado los protocolos y estándares establecidos por el ente rector del sistema nacional de seguridad digital para prevenir, reportar y resolver incidentes de seguridad digital, en los tiempos establecidos en el reglamento de la presente ley. b) No haber implementado los instrumentos del sistema nacional de seguridad digital. c) Entregar fuera de plazo la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de seguridad digital. d) Entregar al ente rector del sistema nacional de seguridad digital información manifiestamente falsa o errónea, cuando ella no sea necesaria para la gestión de un incidente de seguridad digital. e) No haber implementado un sistema de gestión de seguridad de la información. f) No haber elaborado o implementado los planes de continuidad operacional y seguridad digital establecidos en el reglamento general a la presente ley. g) No informar inmediatamente al ente rector del sistema nacional de seguridad digital y a los potenciales afectados sobre la ocurrencia de amenazas, riesgos, incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos. h) No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de una amenaza, riesgo, incidente de seguridad digital o un ciberataque. i) Negarse injustificadamente a cumplir una instrucción del ente rector del sistema nacional de seguridad digital o contradecir el ejercicio de sus atribuciones durante la gestión de un incidente de seguridad digital, siempre que la atribución no cuente con una sanción especial; y, j) La reincidencia en una infracción leve dentro del pazo de seis meses contados desde su cometimiento. • Se sugiere incluir un nuevo artículo, referente a: De las

Remitente Fecha documento	Síntesis de observaciones
	faltas gravísimas. Para efectos de la presente ley se consideran faltas gravísimas las siguientes acciones u omisiones cometidas por personas naturales o jurídicas, públicas o privadas, nacionales o extranjeras: a) Entregar al ente rector del sistema nacional de seguridad digital información manifiestamente falsa o errónea, cuando ella sea necesaria para la gestión de un incidente de seguridad digital. b) Incumplir injustificadamente las instrucciones generales o particulares impartidas por el ente rector del sistema nacional de seguridad digital durante la gestión de un incidente de impacto significativo, de conformidad a lo establecido en el reglamento a la presente ley. c) No entregar la información que se la requiera cuando ella fuere necesaria para la gestión de un incidente digital de impacto significativo; y, k) La reincidencia en una infracción grave dentro del plazo de seis meses contados desde su cometimiento. • Incluir un nuevo artículo: Del Procedimiento Administrativo Sancionador. El procedimiento administrativo se regirá por lo prescrito en el Código Orgánico Administrativo, en la presente ley y su reglamento, que establecen las bases de los procedimientos administrativos que rigen los actos de los organismos de la administración del Estado. • Incluir un nuevo artículo: De los recursos. En contra de la resolución de la máxima autoridad el ente rector del sistema nacional de seguridad digital, mediante la cual se concluye el procedimiento administrativo, procederá el recurso extraordinario de revisión en los casos previstos en la ley, o, en su defecto, procederá la impugnación judicial correspondiente ante los tribunales distritales de lo contencioso administrativo. La interposición del recurso extraordinario de revisión suspenderá el término para reclamar la ilegalidad de la resolución, siempre que se trate de materias por las cuales procede dicho recurso. • Incluir un nuevo artículo: Forma de pago de las multas. Las multas deberán pagarse dentro de los 30 días siguientes contados desde que el acto administrativo que las impone quede firme. Vencido ese plazo, la resolución que establezca la sanción tendrá mérito ejecutivo. El ente rector del sistema nacional de seguridad digital deberá ejercer las acciones de cobro correspondientes a través del procedimiento coactivo previsto en el Código Orgánico Administrativo. El pago de toda multa deberá ser acreditado ante el fondo para la seguridad digital sistémica, dentro de los diez días siguientes a la fecha en que ésta debió ser pagada. • Incluir un nuevo artículo: Pronto pago. El infractor que no interponga recurso alguno podrá, dentro del término de quince días siguientes de que le haya sido notificada la

Remitente Fecha documento	Síntesis de observaciones
	resolución de la máxima autoridad del ente rector del sistema nacional de seguridad mediante la cual se le impone la sanción, pagar directamente en la cuenta única del tesoro nacional. En este caso el monto de la multa impuesta será reducido en un quince por ciento. Una vez ejercido este derecho, se entenderán renunciados todos los recursos administrativos y/o judiciales. • Incluir un nuevo artículo referente a: De la impugnación en sede judicial. La resolución expedida por la máxima autoridad del ente rector del sistema nacional de seguridad digital podrá ser impugnada directamente en sede judicial ante los tribunales distritales de lo contencioso administrativo en observancia al procedimiento ordinario establecido en el Código Orgánico General de Procesos. • En la disposición general segunda, se sugiere cambiar la palabra cibernética por digital. • En la disposición reformatoria segunda, agréguese en el Código Orgánico Monetario y Financiero en su artículo 62, funciones. La Superintendencia de Bancos tiene las siguientes funciones: 9. Exigir a las entidades bajo su supervisión que presenten y apliquen medidas correctivas y de saneamiento apropiadas, especialmente en casos de delitos informáticos y tecnológicos, así como imponer sanciones en caso de incumplimiento de políticas de seguridad digital. • En la disposición reformatoria tercera, se sugiere: agréguese en la Ley Orgánica de la Economía Popular y Solidaria, en el artículo 147, atribuciones. La Superintendencia tendrá las siguientes atribuciones: e. Exigir a las entidades bajo su supervisión que presenten y apliquen medidas correctivas y de saneamiento apropiadas, especialmente en casos de delitos informáticos y tecnológicos, así como imponer sanciones en caso de incumplimiento de políticas de seguridad digital (...). i. Las demás previstas en la ley y su reglamento. • En la disposición transitoria segunda y tercera se sugiere cambiar plazo por término.
Doctor César Antonio Martín Moreno, ministro de Telecomunicaciones y de la Sociedad de la Información. Oficio Nro. MINTEL-MINTEL-2024-0007-O Quito, D.M., 10 de enero de 2024	Presenta varias observaciones al proyecto de ley, entre las que se pueden resaltar de una compilación de varias instituciones: • Subsecretaría de Gobierno Electrónico y Registro Civil. • Subsecretaría de Fomento de la Sociedad de la Información y Economía Digital. • Subsecretaría de Telecomunicaciones y Asuntos Postales. • Dirección Nacional de Datos Públicos. • Dirección General de Registro Civil Identificación y Cedulación. • Agencia de Regulación y Control de las

Remitente Fecha documento	Síntesis de observaciones
	Telecomunicaciones (Arcotel).
Abogada Mónica Fernández Campero, Abogados digitales 4.0. S/O, de 26 de enero de 202024	Presenta observaciones a 9 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 5: Definiciones: - Trazabilidad: Sugerimos tomar la definición otorgada por la Organización Internacional para la Estandarización ISO 9000 como la capacidad de rastrear la historia, la aplicación o la ubicación de lo que está bajo consideración ISO (2005). *Agregar en ataque: ataque informático o ciberataque. *Agregar la definición de: - Sistema Nacional de Seguridad Digital (artículo 26 1° párrafo). - Comité Nacional de Seguridad Digital (artículo 32). - Centro de Respuesta a Incidentes de Seguridad Digital (artículo 39): Es la entidad única y centralizada con competencia para la gestión integral de incidentes digitales. - Incidente de Seguridad: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de la información de una empresa u organismo (no se encuentra en el artículo). • Del artículo 13 al 21: no es necesario colocar el enfoque en el articulado de la norma, quizás en la exposición de motivos o fundamentos para su tratamiento si. Sin perjuicio, que estén implícitos en cada una de los subsistemas y/o comité, u organismos que se generen para el cumplimiento de la seguridad digital. • Del artículo 22 al 25: o lo incorporamos dentro de la sección tercera, gestión de incidentes de seguridad digital o lo suprimimos porque hace al procedimiento y/o protocolo del CERT. Se torna repetitivo. • En el artículo 26 (*recordar que el primer párrafo, se agregó al artículo 5 de definiciones). Artículo 26: Sistema nacional de seguridad digital: Crease el sistema nacional de seguridad digital, cuyo fin será promover la seguridad digital mediante la prevención, gestión e investigación de las amenazas, riesgos y delitos de naturaleza digital que afectan 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. • (*Recordar que la definición del artículo se agregó al artículo 5). Artículo 32: Comité Nacional de Seguridad Digital: Créase el Comité Nacional de Seguridad Digital quien será 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. • En el artículo 76, difícil cumplimiento. (Falta suscripción

Remitente Fecha documento	Síntesis de observaciones
	de Convenio de Budapest). Muchas veces los ciberdelitos no se encuentran regulados en la ley. Otro supuesto es que su investigación no procede por distintos motivos, a veces, por falta de equipos tecnológicos en los organismos competentes para investigación, otras por ser delitos de poca cuantía priorizando a causas más graves (en este caso se las archiva; y otras veces, por falta de preservación de pruebas digitales: ejemplo: la víctima elimina o bloquea la plataforma digital desde donde provino el ciberataque, no se puede investigar.
Ingeniero Oswaldo Roberto Ramos Ferrusola, director general de la Aviación Civil, encargado Oficio Nro. DGAC-DGAC-2024-0302-O, de 02 de febrero de 2024 de 2024 la comisión	Presenta observaciones a 23 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • Sobre los considerandos o Debe revisarle que al final de cada considerando se inserte un punto y coma. o En el séptimo considerando, primera línea, falta agregar después de la palabra: establece, que la. o En el último considerando, primera línea, se repite la palabra señala, por lo que se recomienda su eliminación. • Antes de entrar al título preliminar, debe incluirse la denominación de la Ley Orgánica de Seguridad Digital. • En el artículo 4 de los principios, en el párrafo segundo del denominado disponibilidad, segunda línea, en lugar de pondrán, debe decir: podrán. • En el artículo 33 de la conformación del Comité Nacional de Seguridad Digital y consta en el numeral 3. La máxima autoridad, la Secretaría General de la administración pública o su delegado permanente; mientras que el numeral 8 se lee: La máxima autoridad de la Secretaría General de la Administración Pública y gabinete de la Presidencia de la República o su delegado permanente; estimamos que, en aras de evitar duplicidad, este aspecto debe ser revisado. • En el artículo 34 de las atribuciones del comité, numeral 1, primera línea, en lugar del artículo definido: la, remplazar por el artículo: el. • En el artículo 36 de la Secretaría del Comité Nacional de Seguridad, debe insertarse la palabra: digital. Nótese que el texto se especifica que el secretario será nombrado de entre las o los servidores de la entidad rectora del sistema nacional de seguridad digital, mientras que en el artículo 33, se establece que: La secretaria o el secretario del Comité Nacional de Seguridad Digital se elegirá entre las máximas autoridades o sus delegados permanentes. Resulta inconsistente, por lo que se recomienda aclararlo. • En el artículo 37 de las funciones de la Secretaría del Comité Nacional de Seguridad Digital, remplazar en el numeral 4, primera línea, la preposición en, por el artículo definido: el. • En el artículo 39 del Centro de Respuesta a Incidentes de

Remitente Fecha documento	Síntesis de observaciones
	Seguridad Digital, debe agregarse al título, después de la palabra centro, la palabra nacional; de igual modo, en su texto. • En el artículo 40 de las funciones del Centro Nacional de Respuesta a Incidentes de Seguridad Digital, en el numeral 7, primera línea, eliminar la vocal e, caso contrario, agregar en su lugar el artículo "el". • En el artículo 44 de las atribuciones del ente rector de la defensa nacional, colocar en el numeral 16, luego de la palabra registro, la preposición de. • En el artículo 47 de las atribuciones del ente rector de seguridad ciudadana, protección interna y orden público en materia de ciberseguridad ciudadana, colocar negrillas en parte de su título. • En el artículo 53 de las atribuciones y funciones del ente rector en materia de relaciones exteriores y movilidad humana, en el numeral 5, primera línea, después de la palabra finalidad, agregar la preposición de. • En el artículo 57 de las atribuciones y funciones de la Fiscalía General del Estado, en el numeral 1, al final de la última línea, agregar la letra l a la palabra digital. De la misma manera, en el numeral 13, primera línea, luego de la palabra implementar, remplazar al por: a. • En el artículo 58 de las atribuciones y funciones de las superintendencias como integrantes del sistema nacional de seguridad digital, en el numeral 3, primera línea, después de la palabra comité, cambiar el artículo el por la; y, en su segunda línea, hay una errata, debiendo sustituirse el término rea por: sea. • En el artículo 61 de los instrumentos del sistema nacional de seguridad digital, colocar al final de cada numeral el punto y coma. • En el artículo 65, colocar en el título: Elaboración de la estrategia de seguridad digital, la palabra nacional, en consonancia con el artículo 64. Se recomienda hacerlo también en su texto. • En los artículos 66 y 67 del proyecto, colocar el nombre completo de los instrumentos del Sistema Nacional de seguridad digital, estos son: Planes sectoriales para la reducción, respuesta y recuperación ante riesgos, amenazas e incidentes digitales; y, planes institucionales para la reducción, respuesta y recuperación ante riesgos, amenazas e incidentes digitales. • En el artículo 69 de las certificaciones, poner en el párrafo segundo un punto final. • Agregar al final del artículo 74, un nuevo artículo referido a otros creados o autorizados por el ente rector del sistema nacional de seguridad digital, con la respectiva redacción, que implicará un cambio en su articulado. • En el artículo 77 de las buenas prácticas para promover

Remitente Fecha documento	Síntesis de observaciones
	el acceso a la verdad de los hechos, en la tercera línea, después de la palabra conforman, cambiar la preposición en por el artículo el. • Disposición reformatoria segunda, en la segunda línea, en lugar de a, debe ir el artículo la. • Disposición reformatoria cuarta, en el final del primer texto, luego de facultades, colocar dos puntos, considerándose que empieza una enumeración. • Disposición transitoria primera, en la primera línea, después del número 120, se recomienda colocar la "s" a la palabra día.
Alex Martínez Ramos, magíster, presidente de la Asociación Ecuatoriana de Ciberseguridad (AECI) Oficio Nro. AECI-2024-0129-OR-001, de 29 de enero de 2024.	De acuerdo con nuestro aporte, consideramos que es necesario la inclusión de los siguientes puntos dentro de la Ley Orgánica de Seguridad Digital: • Enfoque en la prevención. • Medidas de protección. • Fortalecimiento del marco legal. • Promoción de la investigación e innovación. • Cooperación internacional. • Gobernanza y transparencia. • Consideraciones adicionales.
Abogado Juan Carlos Larrea Valencia, procurador general del Estado Oficio No. 05315, de 24 de enero de 2024	Con el antecedente de que, en el año 2001, el Consejo de Europa decidió abrir a la firma el convenio sobre delitos cibernéticos (también conocido como Convenio de Budapest), el cual hasta la fecha sigue siendo uno de los principales tratados internacionales destinados a intensificar la cooperación internacional. El objetivo del convenio es aplicar una política penal común para proteger a la sociedad contra la ciberdelincuencia, especialmente mediante la adopción de legislación adecuada y la mejora de la cooperación internacional. Aunque el Estado ecuatoriano no ha suscrito este convenio, muchos de los conceptos y configuraciones de conductas relacionados con la comisión de delitos cibernéticos pueden ser aprovechados para el ejercicio legislativo en Ecuador, como se evidencia en el proyecto de ley analizado. La estratificación jerárquica que ostentará el proyecto, en caso de aprobarse, proporcionará mayor solidez a los conceptos y configuraciones de conductas especializadas, incluso sobre otros cuerpos legales de menor jerarquía, que establezcan enunciaciones distintas o contradictorias. El Global Risk Report 2023, el informe más reciente del Foro Económico Mundial revela la necesidad de establecer mecanismos para prevenir la amenaza global del ciberdelito. Uno de los aspectos más necesarios para este fin es la cooperación interinstitucional y la armonización de normativas afines para facilitar la identificación de debilidades tanto en el ámbito público como privado, siendo este el principal factor de riesgo. Con

Remitente Fecha documento	Síntesis de observaciones
	base en lo expuesto, se considera prudente incluir a la Procuraduría General del Estado como uno de los integrantes fundamentales del sistema nacional de seguridad digital, tal como se establece en los artículos 26 y 27 del proyecto de ley en análisis. Esta inclusión se justifica por el enfoque proactivo de la Procuraduría en la prevención de delitos de naturaleza digital que puedan afectar la seguridad integral del Estado y los derechos de sus ciudadanos en el ciberespacio, sistemas informáticos y redes. La propuesta de modificación al artículo 27 del proyecto sería la siguiente: Artículo 27. Integración del sistema nacional de seguridad digital. El sistema nacional de seguridad digital estará integrado por las siguientes instituciones y organismos: (...) La Procuraduría General del Estado; (...).
Señor magíster electronaurógrafo Jorge Raúl Carrillo Tutiven, secretario de Gestión de Riesgos Oficio Nro. SGR-SGR-2024-0036-O, Samborondón, 10 de enero de 2024	En virtud de los criterios técnicos institucionales, se presentan las siguientes observaciones: 1. Respecto al Proyecto de Ley Orgánica de Seguridad Digital, que trata temas de ciberseguridad ciudadana, ciberdefensa, ciberinteligencia y ciberdiplomacia, debido a la utilización de redes y sistemas de información que se está generalizando de manera acelerada en nuestro país así como en el mundo entero; y cuya digitalización y conectividad se están convirtiendo en elementos esenciales de un número cada vez mayor de productos y servicios; la gestión de riesgos e incidentes en el ciberespacio, deberá analizar, evaluar y catalogar sus activos de información, incluyendo sus vulnerabilidades, amenazas y riesgos. Esta entidad considera que todo aquello no tiene efectos vinculantes con la naturaleza de la Secretaría de Gestión de Riesgos, por lo que al no tener competencia y/o injerencia en el Proyecto de Ley Orgánica de Seguridad Digital, no presentamos observaciones al documento remitido.
Magíster María Gabriela Ochoa Ochoa, directora general del Servicio Nacional de Aduanas del Ecuador Oficio Nro. SENAE-SENAE-2024-0016-OF. Guayaquil, 11 de enero de 2024	Presenta observaciones a 6 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 1, incluir el subsistema ciberdelitos. Lo sugiere el subsecretario del Ministerio de Telecomunicaciones en la Sesión Nro. 132 el 15 de junio del 2022 a la comisión general. • En el artículo 2, corregir literal: d. Derechos humanos del usuario que es víctima de un ciberdelito. • En el artículo 31, se sugiere que también se integre la función de la capacitación y retroalimentación constante sobre ciberseguridad tanto a los usuarios internos como externos. • En el artículo 65, esclarecer sobre el término bianual indicando cada cuánto tiempo realizarán la reformulación de la estrategia. • En la disposición transitoria primera, corregir: 120 días.
Brigadier general	Presenta observaciones a 10 artículos al proyecto de ley,

Remitente Fecha documento	Síntesis de observaciones
(SP) Luis Eduardo Zaldumbide López, director general SNAI Oficio Nro. SNAI-SNAI-2024-0111-O, de 24 de enero de 2024	entre las que se pueden resaltar las siguientes: • En el artículo 5, al definir el ciberdelito se debería considerar que no solo es un acto típico, antijurídico y culpable, sino también punible, puesto que hay que entregar los elementos del delito a los administradores de justicia para que puedan aplicar los procedimientos penales que correspondan. • En el artículo 7, es necesario que se realice el análisis del alcance de la protección de las infraestructuras críticas y estratégicas privadas, pues, conforme la definición de infraestructura crítica, se entendería que son aquellas en las que el Estado ejerce soberanía, pero queda la duda de cómo se va a proteger las infraestructuras estratégicas privadas, y los mecanismos para hacerlo. O si, por el contrario, se va a exigir ciertos controles que los privados deban implementar para la protección. • En el artículo 16, es necesario definir cómo va a ser la inclusión de los sectores privado y comunitario en las políticas públicas, puesto que las políticas públicas se formulan por los entes rectores. Sería importante aclarar si en el proceso de construcción de política pública se va a contar con dichos sectores y la manera en que participarán, para dotar de un componente de participación. Lo propio ocurre con los planes, proyectos y acciones, pues dependiendo de quién los formule, tienen procesos de construcción distinto. • En el artículo 18, respecto del tratamiento y la recopilación de datos, es necesario que se analice la real ponderación de contar con una causa judicial o investigación, puesto que existen instituciones públicas y privadas que almacenan datos, sea por disposición legal o por autorización de la persona, y es necesario que se determine el alcance de los requerimientos judiciales en la recopilación de datos. • En el artículo 20, a fin de guardar armonía con el artículo 225 de la Constitución de la República, se recomienda sustituir la frase diferentes niveles de gobierno del régimen seccional descentralizado por la frase entidades que integran el régimen autónomo descentralizado. • En el artículo 31, el numeral 12 le otorga al actual Ministerio de Telecomunicaciones y Sociedad de la Información la atribución de crear e institucionalizar el observatorio del ciberespacio para recopilar, analizar y clasificar la información sobre amenazas e incidentes. Esta atribución requiere ser revisada con el nivel de clasificación que tendrá esta entidad, pues debería ser agregada en el artículo 15 de la Ley Orgánica de Transparencia y Acceso a la Información Pública o incluirse como un organismo de seguridad al amparo de la Ley de Seguridad Pública y del Estado. De igual

Remitente Fecha documento	Síntesis de observaciones
	manera, se le dispone en el numeral 13 que diseñe y ejecute los programas nacionales de sensibilización y cultura en materia de seguridad digital, sin embargo, se recomienda que el Ministerio rector pueda coordinar estas estrategias, que bien pueden ser propuestas por privados o por otras entidades. Finalmente, en el numeral 26 se deriva tener atribuciones y competencias a un reglamento, lo cual se contrapone con el principio de legalidad. En este sentido, se recomienda indicar que "las atribuciones determinadas en el artículo 31 serán desarrolladas en el Reglamento", más no que por reglamento se incrementen. • En el artículo 34, en el numeral 9 se recomienda revisar el procedimiento de declaratoria de zonas de seguridad al amparo de la Ley de Seguridad Pública y de Seguridad. En el numeral 19 se debe aclarar cuál es la ley de la materia, pues se tiene dos normas, la Ley de Seguridad Pública y del Estado y la Ley Orgánica de Transparencia y Acceso a la Información Pública. Incluso en esta última, el artículo 15 determina que la reserva es por 10 años (artículo 16), es decir, es mayor al de la Ley de Seguridad Pública y del Estado (artículo 19). En el numeral 28 se deriva tener atribuciones y competencias a un reglamento, lo cual se contrapone con el principio de legalidad. En este sentido, se recomienda indicar que las atribuciones determinadas en el artículo 31 serán desarrolladas en el reglamento, más no que por reglamento se incrementen. • En el artículo 36, para el cumplimiento de esta disposición, se deberá contar con un servidor público que sea de carrera. En este sentido, sería importante que se tenga un pronunciamiento del ente a cargo, pues no podría ser una persona con contrato de servicios ocasionales por la estabilidad de los 5 años renovables. • En el artículo 48, el artículo crea una confusión respecto de la conformación del subsistema de ciberinteligencia, pues en inteligencia se habla de subsistemas no de unidades, y para evitar una errónea aplicación de la ley, se recomienda mantener una redacción armónica con las leyes vigentes para evitar entender que se trata de áreas o espacios distintos. • En la disposición transitoria segunda, revisar el tiempo que se otorga, especialmente porque las políticas públicas tienen tiempos superiores a 180 días para su ejecución.
Economista Damián Alberto Larco Guamán, director general Servicio de Rentas Internas	Presenta observaciones a 40 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 4, cambiar la palabra "vigente" por "vigentes". En el principio cooperación, cambiar la palabra "respecto" por "respeto". En el principio disponibilidad, cambiar la palabra "pondrán" por

Remitente Fecha documento	Síntesis de observaciones
Oficio No. NAC-DNJOGEC24-00000004, de 06 de febrero de 2024	"podrán". En el principio oportunidad, cambiar la palabra "los amenazas" por "las amenazas". En el principio reserva de la información, cambiar la palabra autoridades por autoridades, sin coma. • En el artículo 5, en la definición de ciberdiplomacia, cambiar la palabra "de las relaciones" por "de relaciones". En la definición de datos informáticos, cambiar la palabra "programadas diseñados" por "programas diseñados". • En el artículo 8, eliminar del texto servicios no esenciales, eliminar la palabra "no". • En el artículo 16, en el texto gestión los riesgos, aumentar la palabra de, quedando como gestión de los riesgos. • En el artículo 20, poner tilde en la palabra articularán, quedando como articularán. • En el artículo 26, no existe una política de seguridad digital; lo que se tiene actualmente es una política de ciberseguridad. • En el artículo 27, cambiar la palabra involucrado por involucrada. • En el artículo 29, en el numeral 5, colocar la primera letra de la palabra digital en mayúscula, quedando como "Digital". • En el capítulo II, entidades de rectoría, coordinación y gestión incidentes digitales, sesión primera, aumentar la palabra de al siguiente texto gestión incidentes, quedando como gestión de incidentes. Adicionalmente, cambiar la palabra sesión primera por sección primera. • En el capítulo II, entidades de rectoría, coordinación y gestión incidentes digitales, sesión primera, en el numeral 9. Colocar la palabra amenaza en plural, quedando como amenazas. • En el capítulo II, entidades de rectoría, coordinación y gestión incidentes digitales, sesión primera, en el numeral 10. Poner tilde en la palabra publica, quedando como pública. • En el artículo 33. Conformación del Comité Nacional de Seguridad Digital. Cambiar la palabra "cibernética" en el texto Comité Nacional De Seguridad Cibernética, por "digital", quedando como Comité Nacional de Seguridad Digital. • En el artículo 34 en el numeral 7, colocar la palabra estratégica en plural, quedando como estratégicas. En el numeral 12, cambiar las palabras ciber espacio, por la palabra ciberespacio. En el numeral 24, colocar la palabra incidente en plural, quedando como incidentes. • En el artículo 37, reemplazar el texto: Además de las que establece la ley deberá cumplir, por el siguiente texto: La Secretaría del Comité Nacional de Seguridad Digital tendrá las siguientes funciones.

Remitente Fecha documento	Síntesis de observaciones
	• En el artículo 39, aumentar la palabra nacional en el siguiente texto: Artículo 39. Centro de Respuesta a Incidentes de Seguridad Digital. El Centro de Respuestas a Incidentes de Seguridad Digital, quedando como: Artículo 39. Centro Nacional de Respuesta a Incidentes de Seguridad Digital. El Centro Nacional de Respuestas a Incidentes de Seguridad digital. • En el artículo 40, en el numeral 6, separar en dos palabras, la palabra cibervulnerabilidades, quedando como ciber vulnerabilidades. En el numeral 9, colocar la palabra sistema para que inicie con mayúscula, quedando como Sistema. • En el artículo 43, cambiar la palabra "ejecutor" por la palabra "rector". • En el artículo 44, en el numeral 2, aumentar la palabra de en el texto comité nacional seguridad digital, quedando como Comité Nacional de Seguridad Digital. En el numeral 6, aumentar la palabra de en el texto finalidad proponer, quedando como finalidad de proponer. En el numeral 8, aumentar la palabra de en el texto finalidad reportar, quedando como finalidad de reportar. En el numeral 16, aumentar la palabra de en el texto registro evaluaciones, quedando como registro de evaluaciones. • En el artículo 45, cambiar la palabra "ciudadana" por "ciudadana". Poner la palabra Ecu en mayúsculas, quedando como ECU-911. • En el artículo 46, cambiar la palabra ejecutor, por la palabra rector. • En el artículo 47, cambiar por el siguiente texto: Artículo 47. Atribuciones del ente rector de la política pública de ciberseguridad ciudadana. • En el artículo 49, cambiar la palabra "ejecutor" por la palabra "rector". • En el artículo 50, determinar si es del sistema nacional de inteligencia o del subsistema de ciberinteligencia. En el numeral 7, cambiar las palabras "ciber espacio" por la palabra "ciberespacio". En el numeral 9, aumentar la palabra de en el texto finalidad proponer, quedando como finalidad de proponer. En el numeral 13, cambiar las palabras "ciber espacio" por la palabra "ciberespacio". • En el artículo 52, cambiar la palabra "ejecutor" por la palabra "rector". • En el artículo 53, en el numeral 5, aumentar la palabra "de" en el texto finalidad proponer, quedando como "finalidad de proponer". En el numeral 5, aumentar la letra "a" en el texto frente amenazas, quedando como "frente a amenazas". Cambiar la palabra "pueda" por "puedan". En el numeral 14 cambiar las palabras "ciber espacio" por la palabra "ciberespacio". • En el artículo 55, en el numeral 6, colocar tilde en la

Remitente Fecha documento	Síntesis de observaciones
	palabra auditoria, quedando como auditoría. • En el artículo 56, en el numeral 4, colocar tilde en la palabra auditoria, quedando como auditoría. Cambiar la palabra las por la, colocar la palabra escuela en plural, quedando como escuelas; definir. • En el artículo 57, en el numeral 1, cambiar la palabra digita, por digital. En el numeral 13, cambiar el texto implementar, al través, por implementar a través. • En el artículo 58, en el numeral 3, cambiar la palabra "rca" por "sea". En el numeral 4, colocar tilde en la palabra auditoria, quedando como auditoría. • En el artículo 59, en el numeral 6 colocar tilde en la palabra auditoria, quedando como auditoría. • En el artículo 60, observación de fondo ya explicada anteriormente. • En el artículo 61, en el numeral l, eliminar las palabras la ley y reemplazar por la palabra el. Adicionalmente, el plan nacional de reducción, respuesta y recuperación ante riesgos, amenazas e incidentes digitales, no existe. Cambiar la palabra riegos por riesgos. En los numerales 2, 3, 7, 12, finalizar la sentencia con punto y coma. • En el artículo 63, en el texto ejecución de plan, cambiar la palabra "de" por "del", quedando el texto como ejecución del plan. • En el artículo 65, aumentar la palabra nacional, quedando como: Artículo 65. Elaboración de la estrategia nacional de seguridad digital. La estrategia nacional de seguridad digital. • En el artículo 66, colocar las primeras letras del texto estrategia nacional de seguridad digital, en mayúsculas, quedando como Estrategia Nacional de Seguridad Digital. • En el artículo 68, colocar la palabra pública en plural, quedando el texto como empresas públicas. • En el artículo 74, en el texto alertar sus usuarios, aumentar la letra a, quedando el texto como alertar a sus usuarios. • En el artículo 77, cambiar la palabra "en" por "el", quedando el texto como que conforman el sistema nacional de seguridad digital. Eliminar la letra a del texto reglamento a general de aplicación de esta ley, quedando como reglamento general de aplicación de esta ley. • En el artículo 78, cambiar la palabra cibernética por digital, quedando el texto como sistema nacional de seguridad digital. • En la disposición transitoria, cambiar la palabra "dia" por "días", quedando el texto como 120 días.
Magister María Belén Mora Villón, intendente general, subrogante.	• En el artículo 3, se sugiere para mejorar compresión en el punto 2: Promover la seguridad digital de las personas naturales y jurídicas tanto públicas y privadas en el ciberespacio u otros entornos digitales mediante la

Remitente Fecha documento	Síntesis de observaciones
Superintendencia de Bancos Oficio Nro. SB-IG-2024-0008-O, de 10 de enero de 2024	gestión integral de riesgos y amenazas. • En el artículo 4, Se sugiere para mejorar compresión en el punto cooperación: Las entidades, personas naturales y jurídicas tanto públicas y privadas dentro del ciberespacio cooperarán para generar mejores condiciones de seguridad digital (...). Se sugiere en el punto de integridad cambiar entidades no autorizadas por entidades. • En el artículo 5, se sugiere mejorar el concepto de auditoría de ciberseguridad. Se sugiere: Es el estudio periódico para la verificación y evaluación de los sistemas, redes e infraestructuras, así como de los controles establecidos para la protección de la información, a través de la cual una entidad puede medir la eficiencia y efectividad de estos. Mejorar el concepto de amenaza. Además, se sugiere incluir: Es un hecho o acontecimiento que aún no ha sucedido, pero que de ocurrir que pudieran derivar en una interrupción de la continuidad de las operaciones y poner en riesgo la información procesada por los diferentes componentes tecnológicos interconectados. Mejorar el concepto de ataque ya que es redundante. Se recomienda ampliar el concepto y no considerarlo solo como una capacidad de las Fuerzas Armadas; la ciberdefensa en un término utilizado a nivel de la infraestructura tecnológica para contener ataques cibernéticos. En la definición de ciberdiplomacia, cambiar del por de relaciones exteriores SB-DER. Se sugiere incluir la definición de sistémica, seguridad digital, incidente, riesgo, resiliencia. • En el artículo 7, se sugiere incluir y mejorar la redacción: La presente ley protege (...) y que pudieran ser vulneradas (...). • En el artículo 8, se sugiere incluir y mejorar la redacción: La presente ley protege (...), privadas, así como 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 la confidencialidad, integridad y disponibilidad de la información y la entrega y calidad de los servicios no esenciales. • En el artículo 9, se sugiere incluir al inicio: La presente ley protege y defiende (...). • En el artículo 10, se sugiere incluir y mejorar la redacción: La presente ley protege los derechos (...), personas ante los riesgos y amenazas que conlleven al cometimiento de ciberdelitos por medio de las tecnologías de la información y comunicaciones. • En el artículo 11, se sugiere incluir al inicio: La presente ley protege y fomenta (...). • En el artículo 12, se sugiere incluir al inicio: La presente

Remitente Fecha documento	Síntesis de observaciones
	ley protege y fomenta (...). • En el artículo 23, 24, 25, se sugiere adecuar en función de los criterios sugeridos en el artículo 22. • En el artículo 26, se sugiere que el nombre de política de seguridad digital definido dentro de la ley guarde consistencia con política nacional de ciberseguridad, en el ámbito de estrategia nacional de ciberseguridad del Ecuador. • En el artículo 30, se sugiere: sesión primera rectoría corregir a sección primera rectoría. • En el artículo 24: 1. Ninguna. 2. Se sugiere que el nombre de Comité Nacional de Seguridad Digital definido dentro de la ley guarde consistencia con Comité Nacional de Ciberseguridad, en el ámbito de estrategia nacional de ciberseguridad del Ecuador. 3. Ninguna. 4. Se sugiere incluir: Expedir normativa y directrices para la supervisión y control en el ámbito de la seguridad digital en coordinación y conforme las competencias de supervisión de los entes de control. 5 a 7. Ninguna. 8. Se sugiere: Reglamentar la realización de auditorías para la seguridad de la información en el ámbito público y privado, en coordinación y conforme las competencias de supervisión de los entes de control. 9 a 26. Ninguna. • En el artículo 34, se sugiere que el nombre de Comité Nacional de Seguridad Digital definido dentro de la ley guarde consistencia con Comité Nacional de Ciberseguridad, en el ámbito de estrategia nacional de ciberseguridad del Ecuador. 1 a 13. Ninguna. 14. Se sugiere aclarar redacción: Conocer y aprobar el informe nacional anual del estado de la seguridad digital en el Ecuador que incluya las medidas de no repetición adoptadas. Los términos de medidas de no repetición no son claros. 13 a 28. Ninguna. • En el artículo 35, se sugiere que el nombre de Comité Nacional de Seguridad Digital, definido dentro de la ley, guarden consistencia con Comité Nacional de Ciberseguridad, en el ámbito de estrategia nacional de ciberseguridad del Ecuador. Se sugiere incluir, forma de votación, voto dirimente, entre otros. • En el artículo 37, se sugiere que el nombre de Comité Nacional de Seguridad Digital, definido dentro de la ley, guarden consistencia con Comité Nacional de Ciberseguridad, en el ámbito de estrategia nacional de ciberseguridad del Ecuador.

Remitente Fecha documento	Síntesis de observaciones
	1 a 9. Ninguna • En el artículo 39, se sugiere: El Centro de Respuestas a Incidentes de Seguridad Digital es la entidad única, centralizada y especializada (...), la vigilancia, prevención, respuesta y recuperación ante incidentes en el ciberespacio, proporcionando análisis periódicos de incidentes y riesgos de ciberseguridad y coordinando la respuesta a nivel nacional. • En el artículo 58, 1 a 2. Ninguna. 3. Se sugiere corregir el error mecanográfico: Brindar colaboración expedita al comité, el ente rector y a los subsistemas del sistema nacional de seguridad digital, cuando así les sea requerido; 4 a 7. Ninguna. • En el artículo 61, se sugiere cambiar: Son instrumentos para la reducción, respuesta y recuperación ante riesgos, amenazas e incidentes las siguientes: por son instrumentos para la gestión de amenazas, incidentes y riesgos, las siguientes: 1 a 2 Ninguna. • En el artículo 62, se sugiere revisar que este artículo no se contrapone con lo establecido en el Código Orgánico Monetario y Financiero, y lo establecido por las juntas de regulación monetaria y financiera en cuanto a la rectoría de supervisión y control de las entidades del sector financiero público y privado en el ámbito de sus competencias. • En el artículo 64, se sugiere que los nombres de Comité Nacional de Seguridad Digital, Plan Nacional de Seguridad Digital, definido dentro de la ley, guarden consistencia con aquellos definidos en la estrategia nacional de ciberseguridad del Ecuador. • En el artículo 68, se sugiere analizar si el INEC es el organismo técnicamente más adecuado para a acreditar operadores, proveedores y sistemas de información y comunicaciones, para ofrecer servicios a empresas públicas o privadas. • En el artículo 78, se sugiere unificar en todo el documento (si aplica) el término sistema nacional de seguridad cibernética por sistema nacional de seguridad digital. • En la disposición general segunda, se sugiere unificar en todo el documento (si aplica) el término sistema nacional de seguridad cibernética por sistema nacional de seguridad digital. • En la disposición transitoria primera, se sugiere corregir día por días. Se sugiere ampliar el plazo, ya que, al existir la estrategia nacional de ciberseguridad del Ecuador, se entendería que esta deber adecuada y estar alineada a la ley orgánica.
Marco Giovanni López Narváez,	• Una vez revisadas las matrices, que contienen tanto el Proyecto de Ley Orgánica de Seguridad Digital; así como

Remitente Fecha documento	Síntesis de observaciones
superintendente - Superintendencia de Compañías Valores y Seguros Oficio No. SCVS-DSC-2024-00000552-O. Guayaquil, 03 de enero de 2024	el Proyecto de Ley para el Control del Espacio Aéreo Nacional, se concluye que no es competencia de este ente de control pronunciarse acerca de dichos proyectos de ley. Al hacerlo, estaríamos extralimitándonos en nuestras atribuciones y facultades legales. En el derecho público, solamente se puede hacer lo que la ley establece. En ese sentido, encontramos que la Carta Magna establece en su artículo 226: Las instituciones 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 (...).
Doctor Danilo Ivanob Sylva Pazmiño, superintendente de Competencia Económica Oficio SCE-2024-008, 10 de enero de 2024	• En el artículo 26 del proyecto de ley revisado, se define al sistema nacional de seguridad digital. La integración de dicho sistema consta en el artículo 27 del proyecto de ley, en cuyo numeral 16, constan: las superintendencias del país. • Las funciones generales de las instituciones del sistema nacional de seguridad digital están determinadas en el artículo 29 del proyecto de ley, en el que se precisa que esas funciones se ejercen en el marco de las atribuciones y competencias de cada entidad y actor del sistema. • Por otra parte, en la sección quinta del proyecto de ley, que trata sobre las entidades auxiliares del sistema nacional de seguridad digital, establece en el artículo 58 las atribuciones y funciones para todas las superintendencias, como integrantes del sistema nacional de seguridad digital, las que en su mayoría se han identificado que son funciones más que atribuciones; encaminadas al cumplimiento de planes, programas, proyectos y al fortalecimiento de la seguridad digital. • El proyecto de ley cuenta con una disposición transitoria (segunda), en la que se otorga un plazo de 180 días contado desde la entrada en vigor de dicha ley, para que las entidades, organismos y actores del sistema, adecúen su normativa secundaria, estrategias, planes y políticas públicas a dicha ley. Sobre este punto, surge una observación, y es que el tiempo establecido en esta disposición transitoria segunda, no se fija acorde con las reglas del COA, por lo que se exhorta a fijar dicho plazo en meses, a fin de que pueda ser contabilizado correctamente.
Sofía Margarita Hernández Naranjo, superintendente de Economía Popular y Solidaria	Presenta observaciones a 11 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 2, se sugiere que en la parte final del texto de este artículo se incluya la frase y demás normativa pertinente, considerando la expedición del Reglamento a Ley Orgánica de Protección de Datos Personales.

Remitente Fecha documento	Síntesis de observaciones
Oficio Nro. SEPS-SGD-2024-00646-OF, de 9 de enero de 2024	• En el artículo 8, se sugiere que en el artículo 5, que trata sobre las definiciones, se incluya una que considere los activos de información. • En el artículo 33, se sugiere revisar los numerales 3 y el 8 en caso de que se refieren a la misma autoridad. • En el artículo 34, se sugiere que en los numerales 16 y 18 se establezca a quién serían dirigidas las +G62 propuestas que se refieren. • En el artículo 36, se sugiere que se incluyan aspectos relacionados con las áreas de conocimiento y experiencia que debería acreditar el secretario del Comité Nacional de Seguridad Digital. • En el artículo 38, se sugiere que se redacte de forma clara el alcance de las disposiciones de este artículo. • En el artículo 58, se sugiere que en el numeral 2 se elimine la palabra definir y la redacción de esta atribución quede de la siguiente forma: Implementar los 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. Se sugiere que se elimine el numeral 6, ya que esta atribución estaría inmersa en el numeral 2 cuando se refiere a programas, los cuales correspondería implementarlos de acuerdo a las directrices del comité. • En el artículo 78, se sugiere que se revise lo relacionado con el sistema nacional de seguridad cibernética, ya que en parte del texto de la propuesta se refiere al sistema nacional de seguridad digital. • En la disposición reformatoria segunda, se sugiere que se revise el contenido del artículo 62 del libro I del Código Orgánico Monetario y Financiero, ya que el mismo cuenta con un numeral 9 que dispone: Exigir que las entidades controladas presenten y adopten las correspondientes medidas correctivas y de saneamiento, incluyendo aquellas relacionadas a prácticas fraudulentas y prohibidas, con el fin de proteger los derechos de los usuarios y/o clientes del sistema financiero nacional; por lo que no sería pertinente el agregar otro numeral 9. • En la disposición reformatoria tercera, se sugiere que revise el contenido del artículo 147 de la Ley Orgánica de Economía Popular y Solidaria, el cual ya cuenta con una letra e); por lo que, lo propuesto en cuanto a agregar esta letra no sería factible. Así mismo, se sugiere que se analice la pertinencia de contar con normas diferenciadas en lo que corresponde a las organizaciones de la economía popular y solidaria, considerando su naturaleza, y como así lo ha previsto el primer inciso del artículo 145 de la Ley Orgánica de Economía Popular y

Remitente Fecha documento	Síntesis de observaciones
	Solidaria, que dispone: Las regulaciones serán expedidas en forma diferenciada tanto para las personas y organizaciones que conforman la Economía Popular y Solidaria, como el sector financiero popular y solidario y se referirán a la protección, promoción e incentivos, funcionamiento y control de las actividades económicas de las personas y organizaciones a las que se refiere esta ley, en coherencia con las regulaciones que emitan otras instituciones del Estado en orden a proteger los derechos de los usuarios y consumidores. • En la disposición transitoria segunda, se sugiere que en la parte final del texto de este artículo a continuación de la palabra vigor, se incluya lo siguiente: Del reglamento general de aplicación a esta ley.
Economista Alan Sierra Nieto, director general de la Unidad de Análisis Financiero y Económico (UAFE) S/O, de 08 de febrero de 2024	Presenta observaciones a 3 artículos al proyecto de ley, entre las que se pueden resaltar las siguientes: • En el artículo 4, se sugiere: considerar en el artículo 4. Principios. Reserva de la información la necesidad de precautelar información como la que mantiene la Unidad de Análisis Financiero y Económico, cuya finalidad, entre otras, es crear, mantener y actualizar, con carácter reservado, una base de datos con toda la información obtenida en el ejercicio de sus competencias y remitir a la Fiscalía General del Estado el reporte de operaciones inusuales e injustificadas con los sustentos del caso. En ese sentido, la (UAFE) queda prohibida de entregar información reservada, bajo su custodia, a terceros. En virtud de lo expuesto, se propone para la definición de reserva de la Información, el texto descrito a continuación: 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 cuyo acceso estuviere expresamente prohibido por una norma legal, preservando la confidencialidad, integridad y disponibilidad de la información, la cual debe ser protegida del acceso no autorizado, uso, divulgación, modificación, destrucción, con el fin de mitigar los riesgos asociados a la gestión de la información física y digital. (...). • En el artículo 29, se sugiere en el artículo 29 numerales 5 y 11 tomar en cuenta la integridad y confidencialidad de la información física y digital; y, las excepciones a la publicidad de información cuando se trate de información reservada. En virtud de lo expuesto, se propone en los numerales 5 y 11: 5. Articular y coordinar acciones con todas las entidades del sistema nacional de seguridad

Remitente Fecha documento	Síntesis de observaciones
	digital para prevenir, reducir, responder y promover la recuperación resiliente ante amenazas, riesgos, incidentes, ataques o crisis digitales; manteniendo la confidencialidad de la información física o digital, de difusión no autorizada. 11. Entregar la información requerida por las entidades de rectoría y regulación, necesaria para garantizar la seguridad digital; excluyendo aquella información que esté sujeta a reserva legal. • 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, siempre que dicha información no tenga carácter de confidencial, reservada, secreta o secretísima, conforme lo dispuesto en leyes orgánicas vigentes, o haga relación a la defensa o seguridad del Estado.

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

2.2.2.3. Mesas técnicas y mesas interinstitucionales para el procesamiento previo al informe para segundo debate. Con la participación de las y los asesores de los asambleístas integrantes de la comisión, se estableció una metodología de mesas técnicas para el procesamiento de las observaciones presentadas al informe para primer debate. Esta metodología consideró varios hitos técnicos para la construcción de un texto preliminar que fue discutido por las y los señores legisladores de la comisión. De esta manera, desde el mes de marzo de 2024 se realizaron cinco mesas técnicas, con la participación de instituciones, academia y expertos en seguridad digital, para revisar el texto borrador del Proyecto de Ley Orgánica de Seguridad Digital, así como también para tratar 17 artículos considerados como posibles nudos críticos. Se analizó cuatro artículos referente al subsistema del sistema nacional de seguridad digital, tres artículos referente a las

entidades de rectoría, coordinación y gestión de incidentes digitales, tres artículos sobre los mecanismos para el acceso a la información verificada para determinar la verdad de los hechos, dos artículos referente a la gestión de riesgos e incidentes digitales, un artículo respecto al régimen sancionatorio y, finalmente, se analizaron las disposiciones reformatorias y transitorias. 2.2.2.4. Sesiones de la comisión especializada permanente. La Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, durante un total de 5 sesiones realizadas previo al segundo debate, socializó, analizó y debatió el presente proyecto de ley. A continuación, se presenta la tabla de sesiones: Tabla 9. Sesiones de la comisión en las que se debatieron los textos, previo al informe para segundo debate. ----

Sesión Fecha	Link	Puntos tratados
Nro. 17, 24 de enero de 2024	https://fb.watch/pXJM7niB-9/	Comisión general: a. Ministerio de Telecomunicaciones y de la Sociedad de la Información; b. Ministerio de Defensa; c. Ministerio de Gobierno d. Ministerio del Interior; e. Centro de Inteligencia Estratégica; f. Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y Adolescentes Infractores; g. Kevin Palacios; h. Efrén Guerrero Salgado; i. Diego Álvarez.
Nro. 19, 26 de enero de 2024	https://fb.watch/pXJHfBK9x0/	Comisión general: a. Procuraduría General del Estado; b. Agencia de Regulación y Control de las Telecomunicaciones; c. Fiscalía General del Estado; d. Unidad de Análisis Financiero; e. Centro de Inteligencia Estratégica; f. Servicio de Rentas Internas; g. Servicio Nacional de Aduanas del Ecuador; h. Abogado Javier Borja; i. Abogada Mónica Fernández; j. Señor Daniel Tenorio; k. Magíster Luis Enríquez.
Nro. 21, 29 de enero de 2024	https://fb.watch/pXJEAcC8EQ/	Comisión general: a. Centro de Inteligencia Estratégica (CIES); b. Secretaría Nacional de Seguridad Pública y del Estado; c. Servicio Integrado de Seguridad (ECU-911); d. Dirección Nacional de Registros Públicos (Dinardap); e. Consorcio de Gobiernos Autónomos Provinciales del Ecuador

Sesión Fecha	Link	Puntos tratados
		(Congope); f. Asociación de Municipalidades del Ecuador (AME); g. Consejo Nacional de Gobiernos Parroquiales Rurales del Ecuador (Conagopare); h. Servicio Nacional de Aduanas del Ecuador; i. Magister Alex Martínez; j. Señor Polo Fabián; k. Señor Juan Carlos Crespo.
Nro. 22, 07 de febrero de 2024	https://fb.watch/qnmn0qXO9i/	Comisión general: a. Víctor Andrés Quishpe de la Unión Nacional de Educadores; b. Jorge Cástulo Guerrón, experto en Seguridad Digital; c. Diego Urbina, gerente de Región Sur de Amazon Web Services; d. Arturo Cabaña, experto en seguridad digital.
Nro. 32, 17 de abril de 2024	https://www.facebook.com/share/v/mpyGcaNknH8a8Bx7/mibextid=WC7FNe	Comisión general: Punto único: Conocimiento, debate y aprobación del borrador del texto del Proyecto de Ley Orgánica de Seguridad Digital.
Nro. 37, 01 de mayo de 2024	https://www.facebook.com/stories/1060918053872/UzpfSVNDOjEzOTcyNTM3Mzc1OTQ2MjE=/?view_single=1&source=shared_permalink&mibextid=W9rl1R/	Conocimiento, debate y aprobación del informe no vinculante para segundo debate del Proyecto de Ley Orgánica de Seguridad Digital.

2.2.2.5. Asistencia de las legisladoras y legisladores de la comisión. A continuación, se agregan las asistencias de las y los señores legisladores, durante el tratamiento del informe para segundo debate del proyecto de ley. Tabla 10. Asistencia de las legisladoras y legisladores diciembre 2023-mayo 2024. ----------

Convocatoria	Nro. 17	Nro. 19	Nro. 21	Nro. 22	Nro. 32	Nro. 37	Total, asistencias
Mes:	Enero 2024			Febrero 2024	Abril 2024	Mayo 2024	
Asambleísta/Fecha	24	26	29	07	17	01	
Inés Alarcón.	P	P	P	P	P	P	Asistencias: 6 Alterno: Ausencias:
Leonardo Berrezueta	P	P	X	P	P	P	Asistencias: 5 Alterno: Ausencias: 1

Diego Matovelle	P	P	P	P	P	P	Asistencias: 6 Alterno: Ausencias:
Alexandra Castillo	P	P	P	P	P	X	Asistencias: 5 Alterno:1 Ausencias:
Alexandra Arce	P	P	P	P	P	P	Asistencias: 6 Alterno: Ausencias:
Xavier Jurado	P	P	P	P	P	P	Asistencias: 6 Alterno: Ausencias:
Otto Vera	P	P	P	P	P	(P) Alterna Karla Ochoa	Asistencias: 6 Alterno: Ausencias:
Rafael Dávila	P	P	P	P	P	(P) Alterna Gabriela Jumbo	Asistencias: 6 Alterno: Ausencias:
Sandra Rueda	P	P	P	P	P	P	Asistencias: 6 Alterno: Ausencias:

2.2.2.1. Detalle votación del texto borrador del Proyecto de Ley Orgánica de Seguridad Digital. La Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, en la Sesión Nro. 032, socializó, analizó, debatió y voto el texto borrador del proyecto de ley, en bloques de 10. A continuación, se presentan las tablas de votación: Tabla 11. Detalle de la votación de los artículos del 1 al 10 del informe. ----------

Nro.	Asambleista	A favor	En contra	Blanco	Abstención
1	Inés Alarcón Bueno	X			
2	Leonardo Berrezueta	X			
3	Diego Matovelle	X			
4	Alexandra Castillo	X			
5	Alexandra Arce	X			
6	Xavier Jurado	X			
7	Otto Vera				
8	Rafael Dávila				
9	Sandra Rueda	X			
Total		7			

Tabla 12. Detalle de la votación de los artículos del 11 al 20 del informe. ----------

Nro.	Asambleísta	A favor	En contra	Blanco	Abstención
1	Inés Alarcón Bueno	X			
2	Leonardo Berrezueta				
3	Diego Matovelle	X			
4	Alexandra Castillo	X			
5	Alexandra Arce	X			
6	Xavier Jurado	X			
7	Otto Vera				
8	Rafael Dávila				
9	Sandra Rueda	X			
Total		6			

Tabla 13. Detalle de la votación de los artículos del 21 al 30 del informe. --

Nro.	Asambleísta	A favor	En contra	Blanco	Abstención
1	Inés Alarcón Bueno	X			
2	Leonardo Berrezueta	X			
3	Diego Matovelle	X			
4	Alexandra Castillo	X			
5	Alexandra Arce	X			
6	Xavier Jurado	X			
7	Otto Vera	X			
8	Rafael Dávila	X			
9	Sandra Rueda	X			
Total		9			

Tabla 14. Detalle de la votación de los artículos del 31 al 40 del informe. ----------

Nro.	Asambleísta	A favor	En contra	Blanco	Abstención
1	Inés Alarcón Bueno	X			
2	Leonardo Berrezueta	X			
3	Diego Matovelle	X			
4	Alexandra Castillo	X			
5	Alexandra Arce	X			
6	Xavier Jurado	X			
7	Otto Vera				

8	Rafael Dávila	X			
9	Sandra Rueda				
Total		7			

Tabla 15. Detalle de la votación de los artículos del 41 al 50 del informe. ----------

Nro.	Asambleísta	A favor	En contra	Blanco	Abstención
1	Inés Alarcón Bueno	X			
2	Leonardo Berrezueta	X			
3	Diego Matovelle	X			
4	Alexandra Castillo	X			
5	Alexandra Arce	X			
6	Xavier Jurado	X			
7	Otto Vera				
8	Rafael Dávila	X			
9	Sandra Rueda	X			
Total		8			

Tabla 16. Detalle de la votación de los artículos del 51 al 60 del informe. ----------

Nro.	Asambleísta	A favor	En contra	Blanco	Abstención
1	Inés Alarcón Bueno	X			
2	Leonardo Berrezueta	X			
3	Diego Matovelle	X			
4	Alexandra Castillo	X			
5	Alexandra Arce	X			
6	Xavier Jurado	X			
7	Otto Vera	X			
8	Rafael Dávila	X			
9	Sandra Rueda	X			
Total		9			

Tabla 17. Detalle de la votación de los artículos del 61 al 90 y las disposiciones generales, transitorias, declaratorias y derogatorias del informe. ----------

Nro.	Asambleísta	A favor	En contra	Blanco	Abstención
1	Inés Alarcón Bueno	X			
2	Leonardo Berrezueta	X			
3	Diego Matovelle	X			
4	Alexandra Castillo	X			
5	Alexandra Arce	X			
6	Xavier Jurado	X			
7	Otto Vera	X			
8	Rafael Dávila	X			
9	Sandra Rueda	X			
Total		9			

3. Base constitucional y legal 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. En relación con el procedimiento parlamentario, la Constitución establece en el artículo 137: Artículo 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: Artículo 61. Del segundo debate. La comisión especializada analizará y, de ser el caso, recogerá las observaciones efectuadas al proyecto de Ley, en el primer debate. Dentro del plazo máximo de noventa días, contado a partir del cierre de la sesión del Pleno, la comisión especializada presentará a la Presidenta o al Presidente de la Asamblea Nacional el informe para segundo debate. La comisión especializada, atendiendo a la naturaleza y complejidad del proyecto de ley, podrá pedir justificadamente a la Presidenta o al Presidente de la Asamblea Nacional, por una sola vez, la prórroga que considere necesaria para presentar el informe correspondiente. La Presidenta o el Presidente de la Asamblea Nacional determinará si concede o no la prórroga, así como el plazo de la misma. La Presidenta o el Presidente, recibido el informe para segundo debate, ordenará por Secretaría General de la Asamblea Nacional, la distribución del informe a las y los asambleístas. El segundo debate se desarrollará, previa convocatoria de la Presidenta o del Presidente de la Asamblea Nacional, en una sola sesión, en un plazo máximo de seis meses desde la recepción del informe. En el caso de negarse el informe de mayoría, el Pleno de la Asamblea, por decisión de la mayoría simple de sus integrantes, podrá decidir la votación del o los informes de minoría. Durante el segundo debate el o la ponente recogerá las observaciones realizadas por el Pleno. En caso de que el proyecto amerite cambios, la o el ponente solicitará a la Presidenta o al Presidente de la Asamblea Nacional, la suspensión del punto del orden del día, a fin de que la comisión analice la incorporación de los cambios sugeridos. Para este efecto, la Presidenta o el Presidente de la comisión respectiva, convocará a la comisión para que en una sola sesión,

analice y apruebe el texto final de votación sugerido, el mismo que será entregado al Pleno de la Asamblea Nacional, en el plazo máximo de ocho días desde el pedido de suspensión del punto del orden del día. Cuando existan cambios en el texto final para votación, el ponente tendrá la obligación de indicar los mismos, previo a la votación. En el caso de que la comisión no tenga mayoría para aprobar o improbar los cambios en el plazo determinado de ocho días, la o el ponente tendrá la potestad de presentar el texto de votación al Pleno de la Asamblea Nacional. Si el texto aprobado por la comisión y que incorpora las observaciones del segundo debate no cuenta con los votos necesarios para su aprobación en el Pleno de la Asamblea Nacional, la o el ponente podrá realizar los ajustes pertinentes y mocionar ante el Pleno de la Asamblea Nacional la aprobación del proyecto de Ley con el nuevo texto, indicando las modificaciones realizadas. Agotado el segundo debate, la votación del texto final del proyecto de ley no podrá exceder el plazo de sesenta días. Se podrá mocionar la aprobación del texto íntegro de la ley, por secciones o artículos. Con el voto favorable de la mayoría absoluta, el Pleno de la Asamblea Nacional, podrá archivar el proyecto de ley. 3.3. Reglamento de las Comisiones Especializadas Permanentes y Ocasionales. El artículo 8 número 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. La Ley Orgánica de la Función Legislativa, en referencia al plazo para la elaboración del informe para segundo debate de los proyectos de ley, determina: Artículo 61. Del segundo debate. La comisión especializada analizará y de ser el caso, recogerá las observaciones efectuadas al proyecto de Ley, en el primer debate. Dentro del plazo máximo de noventa días, contado a partir del cierre de la sesión del Pleno, la comisión especializada presentará a la Presidenta o al Presidente de la Asamblea Nacional el informe para segundo debate (...). Por lo expuesto, las comisiones especializadas permanentes u ocasionales tienen la obligación de presentar el informe para segundo 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. La presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, mediante Memorando Nro. AN-CSIS-2024-0027-M, de 16 de enero de 2024, solicitó una prórroga de noventa días para presentar el informe para segundo debate del Pleno de la Asamblea Nacional, dado al Decreto Ejecutivo Nro. 741, de 17 de mayo de 2023, por parte del expresidente de la república Guillermo Lasso Mendoza, en la que decreta: "Articulo 1. Disolver a la Asamblea Nacional por grave crisis política y conmoción interna, de conformidad con el artículo 148 de la Constitución de la República del Ecuador. Articulo 2. Notifíquese al Consejo Nacional Electoral para que se convoque a elecciones dentro del plazo de siete días de conformidad con lo establecido en el inciso tercero del artículo 148 de la Constitución de la República y que se notifique a la Asamblea Nacional la terminación de pleno derecho los períodos para los cuales fueron designados las y los asambleístas (...)". Mediante Memorando Nro. AN-SG-2024-0204-M, de 17 de enero de 2024, la prosecretaria general, abogada María

soledad Rocha Diaz, pone en conocimiento que, en virtud del artículo 61 inciso tercero de la Ley Orgánica de La Función Legislativa, se autoriza una prórroga de noventa (90) días para entregar el informe de segundo debate del Proyecto de Ley Orgánica de Seguridad Digital. Mediante Resolución CAL-HKK-2023-2025-0160, de 7 de marzo de 2024, el ingeniero Henry Kronfle Kozhaya, presidente de la Asamblea Nacional, resuelve: "Artículo 1. Declarar receso parlamentario desde el día 26 de marzo de 2024 hasta el 09 de abril de 2024 (inclusive), para las y los asambleistas principales y alternos de la Asamblea Nacional; así como para las sesiones del Pleno; de las Comisiones Especializadas Permanentes y Ocasionales; reuniones de Grupos Parlamentarios Temáticos y Grupos Interparlamentarios de Amistad; del Comité de Ética; y para toda actividad legislativa; (...). Artículo 5. Durante el decurso del receso parlamentario, los plazos o términos de los trámites ordinarios para la aprobación de leyes; sustanciación de solicitudes de juicio político; tramitación de amnistía, indultos, quejas, denuncias; enmiendas y reformas parciales a la Constitución; proceso de seguimiento y evaluación a leyes; y demás trámites, procesos y/o ejercicio de las funciones y atribuciones constitucionales y legales de la Asamblea Nacional y sus órganos, se suspenderán. (...)". En tal virtud, la comisión debe entregar el informe de segundo debate del Proyecto de Ley Orgánica de Seguridad Digital, hasta el 03 de mayo de 2024. Por lo expuesto, la comisión ha cumplido con el plazo legal y reglamentario para la entrega del presente informe. 5. Análisis y razonamiento realizado por los miembros de la comisión en la elaboración del informe para segundo debate. 5.1. Estándares y organizaciones internacionales en materia de seguridad digital. Los estándares y organizaciones internacionales en materia de seguridad digital son fundamentales para promover la seguridad en la era digital. Ayudan a establecer normas,

fomentar la colaboración, proteger la privacidad de los datos, responder a los riesgos, amenazas, incidentes y ciberataques y educar a las personas sobre las mejores prácticas de seguridad. Su importancia evoluciona a medida que la tecnología avance y los riesgos cibernéticos se vuelvan más complejos. 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. La primera es una norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (SGSI). Mientras que, la norma ISO/IEC 27002, proporciona directrices detalladas para la implementación de controles de seguridad de la información. Por lo que, la adopción de estos estándares ayuda a una organización a identificar y protegerse contra posibles amenazas, riesgos e incidentes digitales, 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. Es un marco de trabajo NIST para mejorar la ciberseguridad de la infraestructura crítica y de la seguridad digital. Además, es orientada para la gestión de riesgos de seguridad cibernética a nivel organizacional, con el propósito de ayudar a las organizaciones a protegerse contra posibles amenazas, riesgos, incidentes y ciberataques, en lo referente a la seguridad de la información. Otro estándar importante en la seguridad cibernética es el CIS Controls, desarrollado por el Centro de Seguridad de la Información

(CIS) en Estados Unidos. Se actualizan regularmente para reflejar las últimas amenazas, riesgos e incidentes, a fin de generar mejores prácticas en seguridad digital. El CIS Control, es utilizado por organizaciones de todo el mundo como una guia para fortalecer su postura de seguridad y mitigar riesgos. En el ámbito de la seguridad cibernética, también existen estándares internacionales como el marco nacional de ciberseguridad de los Estados Unidos, que proporciona un conjunto de estándares, pautas y mejores prácticas para ayudar a las organizaciones a gestionar y reducir el riesgo cibernético de manera efectiva. Se basa en los principios de gestión de riesgos, incluyendo identificación, protección, detección, respuesta y recuperación, y ha sido adoptado por muchas empresas y organizaciones en todo el mundo. Es utilizado por una amplia gama de organizaciones en los Estados Unidos, desde empresas privadas hasta agencias gubernamentales, como una herramienta para fortalecer sus defensas cibernéticas y proteger sus activos digitales contra amenazas cada vez más sofisticadas. Por otro lado, a nivel convencional, la seguridad digital no tiene un marco de regulación único, al contrario, existe una pluralidad de normas de mayor o menor complejidad técnica, a las que se suman una serie de instrumentos de soft law como estándares, normativas, pronunciamientos, principios o recomendaciones no vinculantes, pero altamente útiles y aplicables, que las organizaciones pueden utilizar para establecer y mejorar sus prácticas de seguridad cibernética. La elección del marco adecuado dependerá de varios factores, como la ubicación geográfica, el sector de la organización y el nivel de riesgo al que se enfrenta. No obstante, se pude destacar el grado de evolución del marco normativo de la Unión Europea que, establece normas y requisitos específicos para el procesamiento de datos personales y tiene importantes implicaciones para la seguridad

cibernética, ya que exige que las organizaciones implementen medidas técnicas y organizativas adecuadas para proteger los datos personales contra el acceso no autorizado y otras amenazas. Además, 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, ha sido ratificado por numerosos países, tanto dentro como fuera de Europa, siendo un instrumento importante para promover la cooperación internacional en la lucha contra el cibercrimen, el cual establece que los Estados partes deben adoptar una serie de medidas legislativas, políticas, la mejora de la cooperación internacional y el fortalecimiento de las capacidades de los Estados para investigar y procesar delitos cibernéticos, 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. La cooperación en seguridad digital a nivel internacional se lleva a cabo, a través de organizaciones privadas o iniciativas técnicas de cooperación y normativas. 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 a su vez otorga las acreditaciones a las entidades que deseen ser reconocidas como parte de esta red. La colaboración entre diferentes partes interesadas es esencial para abordar los desafíos cada vez más complejos de la seguridad cibernética en un entorno globalizado. Otra de las comunidades de cooperación que existen a nivel internacional es el Trusted Introducer TF-CSIRT2, conformado por una red de equipos de seguridad y respuesta ante incidentes informáticos en todo el mundo, es una iniciativa que surgió en Europa, 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, promoviendo las mejores prácticas en la gestión de incidentes de seguridad. De igual manera, a nivel internacional, existe un marco referencial que sirve de orientación para que los países puedan desarrollar su normativa local. Por otra parte, la Unión Internacional de las Telecomunicaciones desempeña un papel crucial en la promoción del desarrollo y la utilización de las TIC a nivel

mundial, facilitando la cooperación internacional y estableciendo estándares para garantizar la interoperabilidad y la eficiencia en el uso de los recursos de telecomunicaciones; por lo que 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. Referente a la formación y capacitación, se llevan a cabo diversas iniciativas y programas para educar a las personas y organizaciones sobre cómo proteger sus sistemas, datos y activos digitales contra riesgos, amenazas e incidentes cibernéticos, así como también se desarrollan 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. Es por esto que la formación y capacitación en seguridad digital son fundamentales para fortalecer la postura en temas de seguridad, en un entorno cada vez más complejo y desafiante. 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, también se llevan a cabo diversas iniciativas y programas para educar a individuos y organizaciones sobre cómo proteger sus sistemas, datos y activos digitales referente a la formación en la materia. La seguridad digital es esencial para proteger los intereses nacionales, garantizar la privacidad y la seguridad de los ciudadanos y, promover un entorno en línea seguro y confiable para el funcionamiento de la sociedad en su conjunto. 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 proporcionan un marco común para la implementación de medidas de seguridad efectivas y la evaluación de la madurez de la seguridad cibernética y requieren ser más amplios, a fin de dar respuesta al problema desde sus múltiples aristas e integrando a todos los actores interesados, permitiendo aprovechar el conocimiento y los recursos de diferentes partes interesadas para mejorar la seguridad digital en su conjunto. 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 su legislación, la cual es fundamental para que el marco institucional del país, que pueda recibir apoyo y contribuir eficazmente a abordar los desafíos relacionados con el desarrollo de tecnologías modernas y emergentes. Esto puede incluir la creación de regulaciones específicas para áreas como la inteligencia artificial, la seguridad digital, la protección de datos y otros temas relevantes en el panorama tecnológico actual. 5.2. Orientaciones en materia de seguridad digital para los parlamentos del mundo. Las orientaciones en materia de seguridad digital para los parlamentos del mundo pueden variar dependiendo de diversos factores, como el nivel de desarrollo tecnológico del país, las amenazas específicas a las que se enfrenta y las regulaciones vigentes. Sin embargo, existen prácticas comunes como la concienciación y capacitación, las políticas y procedimientos de seguridad, la protección de datos, el control de acceso y autenticación, respuesta ante incidentes, entre otros. 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 10 principios rectores para la ciberseguridad ciudadana. Este instrumento tiene como principal objetivo dotar a las y los parlamentarios, sus equipos 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 requieren garantizar la seguridad digital en los parlamentos y en la comunidad internacional en general, generando convergencia y confianza digital, permitiendo la innovación en sus esfuerzos para garantizar el ejercicio de una ciudadanía digital plena, promoviendo una gobernanza inclusiva y multilateral. Esto principios son el resultado de un esfuerzo entre legisladoras y legisladores, asesores parlamentarios, expertos del sector privado en los campos de la seguridad digital y la transformación digital, así como de académicos y líderes de sociedad civil. Las finalidades de estos principios rectores es proporcionar un marco sólido para abordar los desafíos de la seguridad digital a nivel ciudadano y promover un uso seguro y responsable de la tecnología digital. Así como también, proteger los derechos y libertades fundamentales de los ciudadanos en el ciberespacio, incluyendo el derecho a la privacidad, la libertad de expresión y otros derechos civiles, garantizar que los ciudadanos mantengan el control sobre sus datos personales y que las decisiones políticas y democráticas no se vean comprometidas por interferencias cibernéticas, dotar de una herramienta coherente, rigurosa y estructurada que les permita a los Estados proporcionar una eficaz inclusión, alfabetización y universalización digital. Buscan, además,

reconocer que la seguridad digital es responsabilidad de todos los actores involucrados, incluyendo ciudadanos, empresas, Gobierno y organizaciones, y promover la colaboración en la protección digital. Así mismo, requieren de 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, los mismos que han sido considerados como guías orientadoras en el proceso de construcción normativa que se propone, a fin de garantizar la seguridad y protección de los ciudadanos en el entorno digital y promover un uso responsable y ético de la tecnología. 5.3. Estado de la ciberseguridad en la región y en el Ecuador. La seguridad digital en América Latina es un tema cada vez más relevante debido al crecimiento constante de la conectividad digital en la región, la misma que ha experimentado un aumento significativo en el acceso a internet y la adopción de tecnologías digitales en los últimos años. Esto ha llevado a un incremento en la cantidad de datos y transacciones en

línea, lo que hace que la seguridad digital sea una preocupación importante. A pesar del crecimiento en la conectividad digital, varios países de América Latina aún enfrentan desafíos en términos de infraestructura de tecnología de la información y recursos limitados para abordar la seguridad digital de manera efectiva. Esto incluye una falta de inversión en tecnologías de seguridad y una escasez de personal especializado en la materia. 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. La implementación de normas y procedimientos de seguridad cibernética, la capacitación de los usuarios sobre buenas prácticas de seguridad en línea y la realización de evaluaciones y pruebas de seguridad para identificar y mitigar vulnerabilidades, son elementos imprescindibles en un entorno adecuado de ciberseguridad, lo anterior derivado de la creciente cantidad de información que se maneja en línea, incluyendo información confidencial de empresas, de los propios usuarios y de las entidades de Gobierno, pudiendo algunas de ellas, en caso de ser

afectadas, representar riesgos de seguridad nacional. De acuerdo con el informe de la Junta Internacional de Fiscalización de Estupefacientes 2023, perteneciente a la ONU, el uso de criptomonedas y el ciberespacio es cada vez más frecuente entre las organizaciones criminales de la región, que se disputan el control de los enormes mercados delictivos de drogas, armas, municiones, explosivos, trata de personas, entre otros, lavando millones de dólares al año, utilizando monedas electrónicas y el ciberespacio para su compunción y ejecución de actividades ligadas con estos ilícitos. 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 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; sin embargo, desde agosto 2022, el Ecuador cuenta, por primera vez, con su estrategia nacional de ciberseguridad (ENC), que permitirá a los ciudadanos acceder a servicios digitales con mayor seguridad y fortalecer la protección de sus datos personales. Además, abre nuevas opciones para generar regulación, a fin de proteger a todos los actores de la sociedad de la ciberdelincuencia y fortalece las infraestructuras tecnológicas de las entidades públicas y privadas. La estrategia nacional de ciberseguridad abarca a todo el país, incluyendo Gobierno nacional, organismos de control, instituciones

judiciales, Gobiernos autónomos descentralizados, empresas privadas, entidades académicas y financieras. Su objetivo es generar un ciberespacio seguro para los ciudadanos, promoviendo agilidad en los procesos y creando confianza a escala internacional para que más empresas inviertan en el país. 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. 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 nuevo e integral marco legal en materia de seguridad digital. La irrupción de tecnologías emergentes, sumado al aparecimiento de COVID-19 y sus medidas de distanciamiento, educación en línea, 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 cómo 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 tiempo, esta situación ha generado mayor dependencia hacia la tecnología, incrementando los riesgos, amenazas, incidentes digitales y ciberataques 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 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. 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. 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. El sector

tecnológico se encuentra entre los objetivos centrales de las políticas industriales, y de una mayor intervención de los Estados. El ritmo de investigación y el desarrollo de tecnologías emergentes continuará durante la próxima década, produciendo avances en inteligencia artificial, computación cuántica y biotecnología, entre otras. Para los países que puedan permitírselo, estas tecnologías proporcionarán soluciones parciales a una serie de problemas emergentes, desde hacer frente a nuevas amenazas para la salud y crisis en la capacidad de atención médica hasta incrementar la seguridad alimentaria y mitigación climática. En todas las economías, estas tecnologías también conllevan riesgos, como la ampliación de la desinformación y la rápida rotación de trabajadores en trabajos cualificados y no cualificados. Sin embargo, este rápido desarrollo y despliegue de las nuevas tecnologías, plantea su propio conjunto de riesgos. Junto con un aumento en los delitos cibernéticos, los intentos de interrumpir las tecnologías críticas serán más habituales, con ataques contra la agricultura y el agua, los sistemas financieros, la seguridad pública, el transporte, la energía, así como los usos domésticos, aéreos y submarinos de infraestructura de comunicaciones. Los riesgos tecnológicos no se limitan únicamente a la actuación de actores deshonestos. La sofisticación del análisis de conjuntos de datos más grandes, permitirá el mal uso de información personal a través de legítimos mecanismos que debilitan la soberanía digital de cada persona y el derecho a la privacidad, incluso en lugares bien regulados, regímenes democráticos. 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 es indispensable la decisión política de todos los niveles de Gobierno para dar el apoyo,

incluyendo el presupuestario, al desarrollo de la seguridad digital 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. 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 2008 mantiene esta distinción entre leyes orgánicas y ordinarias. En su artículo 133 establece que serán leyes orgánicas: (i) las que regulen la organización y funcionamiento de las instituciones creadas por la Constitución; (ii) las que regulen el ejercicio de los derechos y garantías constitucionales; (iii) las que regulen la organización, competencias, facultades y funcionamiento de los gobiernos autónomos descentralizados; y, (iv) las relativas al régimen de partidos políticos y al sistema electoral. Al establecer un ámbito competencial exclusivo de las leyes orgánicas, las normas que se refieren a otros aspectos no pueden ostentar este carácter. Dicho artículo añade que la expedición, reforma, derogación e interpretación con carácter generalmente obligatorio de las leyes orgánicas, requerirá mayoría absoluta de los miembros de la Asamblea Nacional. Por otro lado, el

artículo 133 señala que todas las demás leyes serán ordinarias y estas no podrán modificar ni prevalecer jerárquicamente sobre las orgánicas. Como se desprende de las normas constitucionales citadas, son dos los elementos que distinguen a las leyes orgánicas de las ordinarias: 1) regulan materias distintas; 2) se rigen por distintos procedimientos de expedición, reforma, derogación e interpretación. 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, incidentes y ciberataques 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 22, y en el artículo 42 establece como atribuciones 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 82 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 postalfabetización 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 en torno al 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 ciberespacio o mediante el uso de las nuevas tecnologías de la información y la comunicación. Así mismo, la comisión discutió qué 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. 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, incidentes o ciberataques 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. 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 7 instituciones principales y 4 entidades auxiliares; y, podrán, además, participar representantes de entidades públicas, de la sociedad civil o de entidades privadas, de organismos relacionados a la seguridad digital y ciudadanos y ciudadanas que se considere necesario convocar por recomendación del Comité Nacional de Seguridad Digital. A su vez, el sistema nacional de seguridad digital se organiza en 4 subsistemas: ciberdefensa, ciberseguridad, 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 al ente rector de seguridad ciudadana, protección interna y orden público. En los actuales y próximos años, los riesgos asociados a la ciberdelincuencia están creciendo de manera exponencial y acelerada. Entendiendo que la actividad criminal ha incrementado su actuación a través de las

herramientas tecnológicas y que estas son actualmente plataformas para el cometimiento de tipos penales nuevos, en pro de la garantía integral de los derechos y del cumplimiento de los principios de seguridad pública, garantizados en la normativa legal vigente; es menester que el ente rector de la seguridad digital sea el encargado de la seguridad ciudadana, orden público y protección interna. De esta manera se podrán generar las acciones necesarias para combatir los delitos cibernéticos o delitos cometidos con uso o por medio de las tecnologías de la información, los cuales pueden ser de carácter transfronterizo y por ello es necesario que mediante el contingente de la cooperación policial a nivel mundial se puedan generar los mecanismos para la prevención y combate a los delitos en el mundo físico, ciberespacio y demás entornos digitales. Con los acontecimientos de ciberinseguridad que se está generando en el mundo, es importante considerar que la mayoría de los delitos que ocurren en el mundo físico pueden ocurrir en el ciberespacio o en entornos digitales y que algunos de los delitos tradicionales (físicos) pueden utilizar las tecnologías como medio de cometimiento del delito. En relación a la seguridad pública, los bienes jurídicos a proteger son la información personal y los datos sensibles, los cuales son inherentes a las personas, o instituciones como centro de protección de los derechos por parte del Estado ecuatoriano, siendo el Ministerio del Interior, la institución del Estado que debe garantizar los derechos de las personas, a través de las políticas públicas para la prevención, apoyo a la investigación, disuasión y respuesta para combatir a la delincuencia y el crimen organizado local y transnacional, apoyado en su eje ejecutor que es la Policía Nacional. En efecto, el Ministerio del Interior desempeña 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. Así mismo, la comisión discutió sobre el rol del sistema nacional de seguridad digital y el rol del Comité Nacional de Seguridad Digital, aclarando por parte de la comisión y de algunos legisladores que, anteriormente no contábamos con una ley y no existía una organización adecuada por parte del Estado ecuatoriano sobre el combate de las amenazas, riesgos, incidentes y ciberataques. Es por ello que esta ley crea el sistema nacional de seguridad digital como un gran paraguas, quien articulará y coordinará junto con los subsistemas e instituciones las estrategias, normativas, planes, programas, políticas y servicios del sector público en todos los niveles del Estado, personas naturales, jurídicas, privadas o comunitarias que definen, coordinan, integran, ejecutan, supervisan, evalúan y controlan el cumplimiento de la política nacional de seguridad digital. Mientras que debajo de este paraguas se encuentra el Comité Nacional de Seguridad Digital como el organismo técnico estratégico de coordinación, transversalización, de ejecución, evaluación de política pública integral de seguridad digital, 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 e incidentes digitales, ciberataques o crisis que se puedan dar en el ciberespacio. Es importante aclarar que esta norma es subsidiara y transversal a otros futuros proyectos de ley en materia de seguridad que articularán al combate del crimen organizado transnacional. Por otro lado, se aclaró la importancia de que formen parte del sistema nacional de seguridad digital el Comando Conjunto de las Fuerzas Armadas y la Comandancia General de la Policía Nacional, debido a que son quienes proporcional información relevante de inteligencia y contrainteligencia, y los diferentes ministerios de seguridad y defensa son quienes delegan a los diferentes comandantes encargados para desempeñar sus funciones de acuerdo a las competencias. 5.6.3. Gestión de riesgos 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 Estados 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. En este sentido, la gestión de incidentes constituye una actividad fundamental para la seguridad digital, y está organizada en procesos principales: 1. Identificación, categorización y priorización de activos de información; 2. Identificación y categorización de vulnerabilidades de los activos de información; 3. Identificación de amenazas; 4.

Relacionamiento de las amenazas frente a los activos de información en función del nivel de vulnerabilidad de los activos de información; y, 5. Respuesta a amenazas, riesgos e incidentes digitales. 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 riesgos, amenazas, incidentes digitales y ciberataques. La respuesta a los riesgos, amenazas, incidentes digitales y ciberataques 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. 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: 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, 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. Desafíos sobre la importancia de la inteligencia artificial en ciberseguridad. Uno de los temas debatidos en la comisión fue referente al control de la ciberseguridad en la inteligencia artificial (IA), la cual es fundamental debido a que los sistemas de IA pueden ser vulnerables a una variedad de ataques cibernéticos, desde ataques de denegación de servicio hasta intrusiones de datos. Es crucial identificar y mitigar estas vulnerabilidades para proteger los sistemas de IA y los datos que manejan. Es por ello que se lo ha considerado en el artículo 5, en definiciones, en razón de que la inteligencia artificial se desarrolla

empleando una o varias técnicas y estrategias que figuran en un conjunto determinado de objetivos definidos por seres humanos, generando información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa. Así mismo, se ha incluido en las atribuciones y funciones del ente rector de las telecomunicaciones y la sociedad de la información la generación de políticas de uso y aplicación de inteligencia artificial dentro del ciberespacio en territorio ecuatoriano y supervisar el desarrollo sostenible de aplicación sobre sistemas algorítmicos de inteligencia artificial y la prevención de los riesgos que puede suponer el uso de esta nueva tecnología. En la actualidad la inteligencia artificial y la ciberseguridad poseen una vinculación cercana, es decir, que son técnicas propias de la inteligencia artificial el poder ser utilizadas para potenciar la seguridad cibernética, así como también fortalecer los procesos, sistemas, productos y servicios de las instituciones, empresas y demás. La detección temprana de amenazas y la prevención de ataques se encuentran entre las aplicaciones más valoradas de la IA en ciberseguridad. Esto se logra gracias a los algoritmos de aprendizaje automático, que permiten analizar una gran cantidad de datos para detectar patrones irregulares que pudieran revelar ataques o actividades maliciosas. Un control de ciberseguridad sólido es esencial para garantizar la seguridad, la integridad y la confianza en los sistemas de inteligencia artificial. Esto implica la implementación de medidas de seguridad tanto en el diseño y desarrollo de los sistemas de IA, como en su implementación y operación continua. Finalmente, la inteligencia artificial está transformando la forma en que protegemos nuestros sistemas y datos contra ciberamenazas. A medida que la IA sigue avanzando, se espera que siga siendo una herramienta valiosa en la ciberseguridad y que se

utilice de maneras aún más avanzadas. Es importante seguir de cerca el desarrollo de la IA en la ciberseguridad y estar preparados para aprovechar sus beneficios mientras se protege contra sus posibles riesgos. 5.6.6. 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 ciberespacio 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 título II, capítulo IV, 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. 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 la creación de un fondo para la seguridad digital sistémica, con el propósito de garantizar la protección y fortalecimiento de los subsistemas digitales en el ámbito nacional. Este fondo estará destinado a financiar proyectos, investigaciones y medidas destinadas a mejorar la seguridad digital sistémica y prevenir amenazas sistémicas en el ciberespacio. El fondo para la seguridad digital sistémica será administrado por la entidad rectora del sistema nacional de seguridad digital, la cual estará encargada de gestionar los recursos de manera eficiente y transparente, en línea con los objetivos establecidos por la presente ley. Los recursos del fondo podrán

provenir de asignaciones presupuestarias, donaciones, cooperación internacional, así como de multas y sanciones impuestas por violaciones a la seguridad digital. Los criterios de asignación de recursos del fondo se determinarán con base en la evaluación de riesgos y necesidades en materia de seguridad digital, así como en la identificación de áreas prioritarias para la prevención y respuesta ante riesgos, amenazas, ciberataques e incidentes en el ciberespacio, conforme al reglamento general a la presente ley. El fondo para la seguridad digital sistémica financiará acciones como: 1. Desarrollo y actualización de infraestructuras de seguridad digital a nivel nacional; 2. Capacitación y formación de profesionales especializados en seguridad digital; 3. Investigación y desarrollo de tecnologías innovadoras para la protección de sistemas digitales; 4. Implementación de políticas y normativas que promuevan la seguridad digital; 5. Desarrollo de una cultura de seguridad digital y la alfabetización digital; 6. Fortalecimiento de la cooperación nacional e internacional en materia de seguridad digital; y, 7. Las que definan en el reglamento de la presente ley. Finalmente, la comisión ha desarrollado en el título II, el capítulo V, referente al régimen de infracciones y sanciones, el cual hace referencia a las responsabilidades administrativas, las mismas que se aplicarán conforme a lo que determine el reglamento general a la presente ley y se emplearán, conforme a las garantías básicas de derecho a la defensa y del debido proceso. Para efectos de la aplicación de las mismas, se ha considerado detallar en el articulado la clasificación de las faltas en: leves, graves y muy graves. Por otro lado, se menciona las sanciones que desarrolla la infracción a los preceptos de la ley, conlleva la imposición de una multa a beneficio del fondo para la seguridad digital sistémica en diferentes escalas. 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. El texto para segundo debate del Proyecto de Ley Orgánica de Seguridad Digital aclara la conformación del sistema nacional de seguridad digital que originalmente estaba conformado por 26 entidades, lo que hacía imposible su funcionamiento práctico, por lo que se vio la necesidad de reducir su conformación a 7 entidades y 4 entidades auxiliares. Además, se mantuvieron las entidades que conforman el comité, aclarando sus atribuciones como órgano ejecutor. Además, luego de un debate exhaustivo, la comisión definió que el ente rector del sistema nacional de seguridad digital debía ser el ente rector de la seguridad ciudadana y el mantenimiento del orden público, es decir, el actual Ministerio del Interior, en razón de que en el ciberespacio la mayor expansión de actividades ilegales se ha dado en relación a los ciberdelitos, por lo cual resulta fundamental que la entidad a cargo de la seguridad ciudadana sea quien lidere la protección ante este tipo de delitos y amenazas cibernéticas. La comisión decidió incluir un capítulo relativo al reconocimiento de los derechos digitales, en el cual se incluyeron los derechos y libertades en los entornos digitales, verificación de identidad, información en el entorno digital y derechos frente al ciberdelito. De esta forma, el Ecuador se coloca una vez más a la vanguardia en el reconocimiento de nuevos y progresivos derechos, tal como lo determina la Constitución de la República. Respecto del fondo, la comisión consideró determinar con claridad las actividades a financiar: proyectos, investigaciones y medidas destinadas a mejorar la seguridad digital sistémica y prevenir amenazas sistémicas en el ciberespacio. Además, se determinó que el fondo será administrado

por la entidad rectora del sistema nacional de seguridad digital y se alimentará de: asignaciones presupuestarias, donaciones, cooperación internacional, multas y sanciones impuestas por violaciones a la seguridad digital. Otro aspecto relevante es el desarrollo de la normativa para regular en términos generales el desarrollo de la inteligencia artificial, a fin de que el ente rector de las telecomunicaciones y la sociedad de la información, sea el encargado de generar políticas para su uso y aplicación, supervisar el desarrollo sostenible de aplicación sobre sistemas algoritmicos de inteligencia artificial y prevenir los riesgos que puede suponer el uso de esta nueva tecnologia. Finalmente, la comisión determinó la necesidad de establecer un régimen sancionatorio, a fin de que la ley tenga una aplicación práctica, al ser exigible mediante la imposición de sanciones. A fin de evitar cualquier vulneración al principio de legalidad, se ha establecido una clasificación de faltas en leves, graves y muy graves, considerando el respecto al debido proceso y el derecho a la defensa. 7. Recomendaciones del informe. Sobre la base del análisis y conclusiones que anteceden, se recomienda la aprobación del informe de segundo debate del Proyecto de Ley Orgánica de Seguridad Digital y que el mismo sea remitido al presidente de la Asamblea Nacional, a fin de que sea distribuido a las y los asambleistas y continúe el respectivo trámite legislativo. 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 segundo debate de la Ley Orgánica de Seguridad Digital. 2. Disponer al señor secretario de la Comisión Especializada Permanente de Soberania, 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 11. Detalle de la votación del informe. ----------

Nro.	Asambleísta	A favor	En contra	Blanco	Abstención
1	Inés Alarcón	X			
2	Leonardo Berrezueta	X			
3	Diego Matovelle	X			
4	Alexandra Castillo				
5	Alexandra Arce	X			
6	Xavier Jurado	X			
7	Karla Ochoa	X			
8	Gabriela Jumbo	X			
9	Sandra Rueda	X			
Total		8			

9. Asambleísta ponente. El asambleísta ponente será la asambleísta Inés Margarita Alarcón Bueno, asambleísta por la provincia de Pichincha y presidenta de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral. 10. Nombre y firma de las y los asambleístas que suscriben el informe. Asambleístas: Inés Alarcón, Leonardo Berrezueta, Diego Matovelle, Alexandra Arce, Xavier Jurado, Karla Ochoa, Gabriela Jumbo, Sandra Rueda. 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. En mi calidad de secretario relator de la Comisión Especializada Permanente de Soberanía Integración y Seguridad Integral y de conformidad a lo que dispone la Ley Orgánica de la Función Legislativa y el Reglamento de Comisiones Especializadas Permanentes y Ocasionales. Certifico: Que, el informe para segundo debate del Proyecto de Ley Orgánica de Seguridad Digital, se conoció, debatió y aprobó en la Sesión ordinaria Nro. 037, de 01 de mayo de

2024, en el pleno de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, con la votación de las y los siguientes asambleístas: Inés Margarita Alarcón, Leonardo Renato Berrezueta Carrión, Diego Fernando Matovelle Vera, Sandra Elizabeth Rueda Camacho, Alexandra Andrea Castillo Campoverde, Alexandra Manuela Arce Plúas, Xavier Andrés Jurado Bedrán, Karla Piedad Ochoa Suárez, Gabriela Nicole Jumbo Quichimbo, con las siguiente votación: ocho (8) a favor, cero (0) en contra, cero (0) abstenciones, cero (0) en blanco; asambleístas ausentes: uno (1). Quito, 01 de mayo de 2024. Lo certifico. Magister Marco Jirón Paredes, secretario relator de la Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral". Hasta ahí la lectura del informe, debiendo recordar, señor presidente, que el mismo, de manera íntegra, será parte del acta de la presente sesión. ----------

EL SEÑOR PRESIDENTE. Se abre el debate. Tiene la palabra la asambleísta ponente Inés Alarcón. ----------

LA ASAMBLEÍSTA ALARCÓN BUENO INÉS. Gracias, señor presidente. Buenas tardes, compañeros asambleístas. Buenas tardes al pueblo ecuatoriano que nos sigue por los diferentes medios de comunicación. Hoy nos encontramos debatiendo el Proyecto de Ley Orgánica de Seguridad Digital, una norma que en primer debate incluía setenta y ocho artículos y actualmente contamos con una norma de noventa artículos, dos disposiciones generales, tres disposiciones transitorias, nueve disposiciones reformatorias y una disposición derogatoria. Este proyecto de ley busca el fortalecimiento de la ciberseguridad, a fin de convertir al país en un referente regional y mundial en materia de seguridad digital y de información. Esta ley mantiene aristas

importantes en la prevención y promoción de la cultura y seguridad digital, también la alfabetización digital. El Ecuador requiere una política de seguridad digital amplia, disruptiva e innovadora, en la cual las personas naturales, empresas públicas y privadas deban adaptarse a las necesidades de seguridad en el ecosistema digital del Ecuador y no viceversa. La presente ley no es estrictamente punitiva, dado que los tipos penales que condenan los delitos informáticos ya se encuentran establecidos en el COIP. Esta ley establece un régimen administrativo que tiene por objeto que la norma no sea letra muerta, sino que en su cumplimiento acarreé consecuencias jurídicas; es decir, una sanción pecuniaria. Esta ley no crea gasto público, pues no crea ninguna institución alterna a las ya existentes, tan solo se crean cuerpos colegiados para determinar, aplicar y supervisar el cumplimiento de la política pública en materia de seguridad digital. Existen casos puntuales en los cuales se pudo evidenciar la falta de transparencia y la necesidad de contar con un cuerpo normativo que regule las obligaciones y las responsabilidades de los prestadores de servicios digitales y de todos los actores. No somos conscientes de las implicaciones que tiene la pérdida de información personal y el mal manejo de la esfera digital. Por otro lado, en el ámbito privado, tampoco están exentos de estas amenazas, riesgos e incidentes digitales. Uno de los objetivos de más alto valor para los ciberatacantes es el sector financiero. Es importante recalcar que esta ley determina claramente las responsabilidades de todos los actores de ciberseguridad en armonía con la Ley de Protección de Datos, no obstante, estas responsabilidades son proporcionales al grado de participación. Actualmente no existe un cuerpo legal que regule estas actividades, por lo cual, es necesario proteger y resguardar los activos informáticos y servicios. Como datos, compañeros asambleístas, en el dos mil

veintitrés, el setenta y dos por ciento de los ecuatorianos tienen acceso a internet, lo que muestra un incremento importante respecto al año dos mil dieciocho, en donde solo era el cincuenta y cinco por ciento. Esto evidencia la necesidad de contar con una ley que regule la ciberseguridad ante el mayor uso de internet que generó la pandemia, de este porcentaje de usuarios, el setenta y nueve por ciento utiliza internet para comunicaciones. Se han incrementado los delitos informáticos, por ejemplo, el acceso no consentido a sistemas informáticos pasó de trescientos cincuenta y tres delitos en el dos mil veintidós a cuatrocientos ochenta y ocho delitos en dos mil veintitrés. Esto refuerza la necesidad de regular este sector. Así mismo, el incremento de uso de TIC para cometer delitos, por ejemplo, la suplantación de identidad, cambió de cinco mil novecientos once casos en el dos mil veintidós a seis mil quinientos veintinueve casos en el dos mil veintitrés. La comisión, mediante veintitrés mesas técnicas, debatió en torno al objeto del proyecto de esta ley su ámbito de aplicación, finalidad y, sobre todo, lo que deberá 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 los derechos humanos. Hemos considerado que el ente rector de este sistema sea el ente rector de la seguridad ciudadana, es decir, el actual Ministerio del Interior, en razón de que el ciberespacio, en la mayor expansión de actividades ilegales se han dado en relación a ciberdelitos; por lo cual, resulta fundamental que la entidad a cargo de la seguridad ciudadana sea quien lidere la protección de este tipo de amenazas cibernéticas. Sin embargo, es importante aclarar que el artículo treinta y siete no otorga ninguna competencia para investigar ciberdelitos al sistema, por lo cual, se están respetando las competencias de la Fiscalía General del Estado. Esto ratificado en el

artículo treinta y nueve, en el cual se determinan las atribuciones del ente rector, el cual, obviamente, no tiene la potestad de realizar ninguna investigación preprocesal ni procesal penal. Así mismo, la Constitución en el artículo trescientos noventa y tres menciona: el ministerio responsable de la seguridad ciudadana, protección interna y orden público, tiene como competencia garantizar la seguridad ciudadana y convivencia. Finalmente, la comisión determinó la necesidad de establecer un régimen sancionatorio para que la ley tenga una planificación práctica al ser exigible mediante la imposición de sanciones, a fin de evitar cualquier vulneración al principio de legalidad. Se ha establecido una clasificación de faltas leves, graves y muy graves, considerando respecto al debido proceso y el derecho a la defensa. Es importante recalcar que esta imposición de sanciones no es arbitraria ni desproporcionada, pues la propia ley establece que se deben tomar en cuenta las acciones que la persona haya emprendido, y las sanciones deben guardar armonía con el tipo de conducta que se busca castigar. Este proyecto de ley coadyuva con la seguridad nacional, y hoy más que nunca es de vital importancia, compañeros, ser parte de una legislación conectada con la realidad en nuestro país. Sin embargo, la Asamblea Nacional, al ser la casa de la democracia y en donde cada uno de nosotros somos los representantes del pueblo ecuatoriano, como comisión nos hemos permitido recibir observaciones. Y le solicitamos, señor presidente, nos permita subir el proyecto de ley ocho días a la comisión para que pueda ser debatido este proyecto de seguridad nacional. Gracias. ----------

EL SEÑOR PRESIDENTE. Señores asambleístas, la asambleísta ponente Inés Alarcón ha solicitado que el informe regrese a la comisión. Por lo tanto, vamos a suspender el debate hasta que llegue el nuevo informe

con las observaciones que estoy seguro que muchos de ustedes van a hacer llegar a la comisión, y ahí retomaremos la sesión y el debate. Por lo tanto, se suspende la presente sesión. Recordemos que tenemos sesión a las dos de la tarde. Muchas gracias. ----------

LA SEÑORA SECRETARIA. Se suspende la sesión siendo las doce horas cincuenta y siete minutos. ----------

V

El señor presidente suspende la sesión cuando son las doce horas cincuenta y siete minutos. ----------

ING. HENRY FRONFLE KOZHAYA
Presidente de la Asamblea Nacional

ABG. MARÍA SOLEDAD ROCHA DÍAZ
Prosecretaria general de la Asamblea Nacional

SVQ/JCC