

15 ABR. 2025
RECIBIDO
Firma: _____ Hora: 10:33 h.

DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY 8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA CREACIÓN DEL COMITÉ DE ALTO NIVEL DE CIBERSEGURIDAD DEL ESTADO PERUANO

COMISIÓN DE CIENCIA, INNOVACIÓN Y TECNOLOGÍA
Período Anual de Sesiones 2024-2025

SEÑOR PRESIDENTE:

Ha ingresado para estudio y dictamen de la Comisión de Ciencia, Innovación y Tecnología, las siguientes iniciativas legislativas:

- **Proyecto de Ley 8842/2024-CR**, presentado por el congresista **Raúl Huamán Coronado**, integrante del grupo parlamentario Fuerza Popular, que propone la "Ley que declara de interés nacional y necesidad pública la creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano".
- **Proyecto de Ley 9906/2024-CR**, presentado por el congresista **Wilson Soto Palacios**, integrante del grupo parlamentario Acción Popular, que propone la "Ley de Seguridad Digital o Ciberseguridad".

En la **DÉCIMA TERCERA SESIÓN ORDINARIA**, celebrada el 31 de marzo de 2025, la Comisión de Ciencia, Innovación y Tecnología, con la dispensa del trámite de sanción del acta para ejecutar los acuerdos, se aprobó por **UNANIMIDAD** el dictamen recaído en los Proyectos de Ley **8842/2024-CR y 9906/2024-CR**. Votaron a favor los señores congresistas: Alfredo Pariona Sinche, Carlos Javier Zeballos Madariaga, George Edward Málaga Trillo, Segundo Héctor Acuña Peralta, Carlos Enrique Alva Rojas, Ernesto Bustamante Donayre, Waldemar José Cerrón Rojas, Miguel Ángel Ciccía Vásquez, Víctor Seferino Flores Ruíz, David Julio Jiménez Heredia, Silvia María Monteza Facho, Karol Ivett Paredes Fonseca y Magally Santisteban Suclupe.

Con la licencia del señor congresista: Abel Augusto Reyes Cam.

I. CONTENIDO DE LAS PROPUESTAS LEGISLATIVAS

- **Proyecto de Ley 8842/2024-CR**: "Ley que declara de interés nacional y necesidad pública la creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano"

El proyecto legislativo plantea un único artículo único de carácter declarativo.

Artículo único. *Declaratoria de interés nacional y necesidad pública la Ley que Declara de Interés Nacional y Necesidad Pública la Creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano.*

DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO

Declárase de interés nacional y necesidad pública la creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano, a fin de implementar herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los datos activos de una organización y de los usuarios de un ciberentorno.

- **Proyecto de Ley 9906/2024-CR: "Ley de Seguridad Digital o Ciberseguridad"**

El proyecto legislativo se encuentra constituido por ocho artículos, dos Títulos, dos Capítulos y dos Disposiciones Complementarias Finales, que disponen entre otros, lo siguiente:

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto de la Ley

La presente ley tiene por objeto establecer el marco normativo de a seguridad digital en el Estado peruano, con el fin de proteger la información digital, dispositivos, activos, incluidos la información personal, cuentas del sistema financiero, archivos, imágenes y el patrimonio del Estado, así como de las personas naturales y jurídicas, frente a ciberataques.

Artículo 2. Ámbito de Aplicación

La presente ley es aplicable a las entidades del sector público en todos los niveles de gobierno. Asimismo, se extiende a las entidades del sector privado, la academia y la sociedad civil, en aquellos aspectos que les correspondan según su naturaleza y funciones.

Artículo 3. Respeto a los derechos humanos en la ciberseguridad

En toda normativa y política relacionada con la ciberseguridad, se deberá garantizar el respeto irrestricto a los derechos humanos, en concordancia con la Constitución Política del Perú y los tratados internacionales suscritos y ratificados por el país.

Artículo 4. Comunicación de incidencias de ciberseguridad

Los mecanismos de comunicación de incidentes entre la sociedad civil, el sector privado, la academia, la comunidad técnica y el sector gubernamental deberá garantizar la confidencialidad de los casos que puedan afectar las instituciones o a la sociedad civil. Cada caso será evaluado para determinar si es pertinente divulgar información a otros actores y a la ciudadanía.

Cuando un incidente implique la violación de datos personales, se deberá notificar al funcionario responsable de transparencia, acceso a la información pública y protección de datos personales.

DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO

Asimismo, se deberá informar a las autoridades competentes según la naturaleza del incidente, las entidades afectadas y las personas involucradas, para que actúen dentro del ámbito de sus funciones.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, será responsable de establecer los protocolos de comunicación, recepción, escalamiento, coordinación, reporte, intercambio y activación frente a incidentes de seguridad digital.

TÍTULO II DE LA CIBERSEGURIDAD

CAPÍTULO I CIBERSEGURIDAD EN EL SECTOR PÚBLICO

Artículo 5. Comité de Ciberseguridad del Estado Peruano

Créase el Comité de Ciberseguridad del Estado Peruano, que operará de ad honorem y estará conformado por representantes del sector público, el sector privado, la sociedad civil, la academia y la comunidad técnica de internet. Este comité estará adscrito a la Presidencia del Consejo de Ministros y contará con la Secretaría de Gobierno Digital como su secretaría técnica, la cual coordinará con el secretario técnico del Consejo de Seguridad y Defensa Nacional (COSEDENA).

El Comité será responsable de formular la Política de Ciberseguridad del Estado Peruano, establecer lineamientos para los equipos de respuesta ante incidentes de seguridad informática, gestionar el Fondo de Seguridad Digital, promover una cultura de ciberseguridad, impulsar la incorporación de contenidos sobre ciberseguridad en los currículos de educación superior y desempeñar otras funciones asignadas por el COSEDENA.

La conformación y el funcionamiento del Comité de Ciberseguridad se definirán en el reglamento de la presente ley.

Artículo 6. Marco de Seguridad Digital en el Sector Gubernamental

La Secretaría de Gobierno Digital será responsable de establecer los principios, modelos, políticas, normas, procesos, roles, tecnologías y estándares mínimos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información en los entornos digitales administrados por las entidades de la administración pública.

CAPÍTULO II CIBERSEGURIDAD EN EL SECTOR PRIVADO

Artículo 7. Lineamientos para los equipos de respuesta frente a incidentes de seguridad informática en el sector privado

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

El Comité ad honorem de Ciberseguridad del Estado Peruano establecerá los lineamientos necesarios para la creación y operación de equipos de respuesta a incidentes de seguridad informática (CSIRT) en el sector privado, la academia, la sociedad civil y la comunidad técnica. Asimismo, promoverá el desarrollo de instrumentos de cooperación público-privada orientados a fortalecer la ciberseguridad en el país.

Artículo 8. Cooperación Público – Privada en materia de ciberseguridad

Las entidades públicas privadas, así como las instituciones académicas, la sociedad civil y la comunidad técnica, deberá establecer sus acciones en el principio de cooperación mutua para garantizar el mantenimiento y fortalecimiento de la ciberseguridad a nivel nacional.

DISPOSICIONES COMPLEMENTARIAS

PRIMERA. Reglamentación en materia de ciberseguridad

La Presidencia del Consejo de Ministros aprobará el reglamento de la presente ley en un plazo máximo de noventa (90) días calendario, contados a partir del día siguiente de su publicación en el Diario Oficial El Peruano.

DISPOSICIÓN COMPLEMENTARIA FINAL

ÚNICA. Vigencia

La presente ley entrará en vigencia al día siguiente de su publicación en el Diario Oficial El Peruano.

II. SITUACIÓN PROCESAL

2.1 Antecedentes

El Proyecto de Ley 8842/2024-CR, fue presentado ante el área de trámite documentario el 9 de setiembre de 2024 y fue decretado a la Comisión de Ciencia, Innovación y Tecnología el 10 de setiembre de 2024 para estudio y dictamen como segunda comisión dictaminadora; y a la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra Las Drogas, como primera comisión dictaminadora.

El Proyecto de Ley 9906/2024-CR, fue presentado ante el área de trámite documentario el 13 de enero de 2025 y fue decretado a la Comisión de Ciencia, Innovación y Tecnología el 14 de enero de 2025 para estudio y dictamen como segunda comisión dictaminadora; y a la Comisión de Descentralización, Regionalización, Gobiernos Locales y Modernización de la Gestión del Estado, como primera comisión dictaminadora.

La Comisión de Ciencia, Innovación y Tecnología (CCIT) ha verificado que las propuestas legislativas cumplen con los requisitos establecidos en los artículos 75 y 76

DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY 8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA CREACIÓN DEL COMITÉ DE ALTO NIVEL DE CIBERSEGURIDAD DEL ESTADO PERUANO

del Reglamento del Congreso de la República, sobre la formalidad de la exigencia del cumplimiento de requisitos para la presentación de propuestas legislativas. La iniciativa reseña una exposición de motivos que describe el problema que se pretende resolver, cuenta con un acápite de los antecedentes legislativos; incluye los efectos de la vigencia de la norma en la legislación nacional, el análisis costo-beneficio; y su relación con las políticas de Estado en el Acuerdo Nacional. Asimismo, cuenta con la firma del portavoz del grupo parlamentario, así como con las firmas correspondientes de los demás congresistas que respaldan la iniciativa de ley.

Por otro lado, la Comisión de Ciencia, Innovación y Tecnología ha verificado que la iniciativa legislativa cuenta con antecedentes parlamentarios, como se detalla a continuación:

Proyecto de Ley	Sumilla
4237/2018-CR	Ley que promueve la seguridad informática en el Perú y la conformación de un Consejo Nacional de Ciberseguridad.
4352/2018-CR	Ley de Ciberseguridad.

2.2 Opiniones solicitadas

Respecto al **Proyecto de Ley 8842/2024-CR**, se han cursado las siguientes solicitudes de opinión:

Fecha	Institución	Documento	Respuesta
19/09/2024	Centro Nacional de Seguridad Digital - PCM	Oficio N° 045-2024-2025-CCIT-CR	-
19/09/2024	Fiscalía de la Nación	Oficio N° 040-2024-2025-CCIT-CR	-
19/09/2024	Poder Judicial	Oficio N° 041-2024-2025-CCIT-CR	-
18/10/2024	Ministerio de Justicia y Derechos Humanos (MINJUSDH)	Oficio N° 113-2024-2025-CCIT-CR	Reiterativo
19/09/2024	Consejo Nacional de Política Criminal (CONAPOC)	Oficio N° 044-2024-2025-CCIT-CR	-
19/09/2024	Ministerio de Justicia y Derechos Humanos (MINJUSDH)	Oficio N° 042-2024-2025-CCIT-CR	Sí
18/10/2024	Ministerio Público – Fiscalía de la Nación	Oficio N° 111-2024-2025-CCIT-CR	Reiterativo
18/10/2024	Consejo Nacional de Política Criminal (CONAPOC)	Oficio N° 115-2024-2025-CCIT-CR	Reiterativo
19/09/2024	Consejo Nacional Penitenciario (INPE)	Oficio N° 043-2024-2025-CCIT-CR	-
19/09/2024	Ministerio del Interior (MININTER)	Oficio N° 038-2024-2025-CCIT-CR	-
18/10/2024	Ministerio del Interior (MININTER)	Oficio N° 110-2024-2025-CCIT-CR	Reiterativo
18/10/2024	Instituto Nacional Penitenciario (INPE)	Oficio N° 114-2024-2025-CCIT-CR	Sí

DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY 8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA CREACIÓN DEL COMITÉ DE ALTO NIVEL DE CIBERSEGURIDAD DEL ESTADO PERUANO

19/09/2024	Policía Nacional del Perú	Oficio N° 039-2024-2025-CCIT-CR	Sí
18/10/2024	Poder Judicial	Oficio N° 112-2024-2025-CCIT-CR	Reiterativo
18/10/2024	Presidencia del Consejo de Ministros	Oficio N° 116-2024-2025-CCIT-CR	Sí

Respecto al **Proyecto de Ley 9906/2024-CR**, se han cursado las siguientes solicitudes de opinión:

Fecha	Institución	Documento	Respuesta
16/01/2025	Ministerio Público – Fiscalía de la Nación	Oficio N° 906-2024-2025-PO-CCCIT-CR	-
16/01/2025	Presidencia del Consejo de Ministros	Oficio N° 902-2024-2025-PO-CCCIT-CR	Sí
16/01/2025	Ministerio del Interior (MININTER)	Oficio N° 903-2024-2025-PO-CCCIT-CR	Sí
16/01/2025	Poder Judicial	Oficio N° 907-2024-2025-PO-CCCIT-CR	-
16/01/2025	Ministerio de Justicia y Derechos Humanos (MINJUSDH)	Oficio N° 905-2024-2025-PO-CCCIT-CR	-
16/01/2025	Asamblea Nacional de Gobiernos Regionales (ANGR)	Oficio N° 901-2024-2025-PO-CCCIT-CR	-
16/01/2025	Ministerio de Defensa (MINDEF)	Oficio N° 904-2024-2025-PO-CCCIT-CR	-
16/01/2025	Consejo Nacional de Ciencia, Tecnología e Innovación (CONCYTEC)	Oficio N° 908-2024-2025-PO-CCCIT-CR	-

2.3. Opiniones recibidas

2.3.1. Proyecto de Ley 8842/2024-CR

Se ha recibido las siguientes respuestas a los pedidos de opinión:

Fecha	Institución	Documento
21/09/2024	Policía Nacional del Perú	Oficio N° 634-2024-CG PNP/SEC
25/10/2024	Presidencia del Consejo de Ministros	Oficio N° D002111-2024-PCM-SG
05/12/2024	Ministerio de Justicia y Derechos Humanos	Oficio N° 4882-2024-JUS/SG
03/12/2024	Instituto Nacional Penitenciario	Oficio N° D001293-2024-INPE-PRE

2.3.1.1 Opinión de la Policía Nacional del Perú.

Mediante Oficio N° 634-2024-CG PNP/SEC, de fecha 21 de setiembre de 2024, el secretario de la Comandancia General PNP pone de conocimiento que con Oficio N° 000391-2024-IN-DM de fecha 20 de setiembre de 2024, el ministro del Interior solicitó al presidente del Congreso, que todos los requerimientos dirigidos a la Policía Nacional

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

del Perú sean dirigidos al Ministerio del Interior.

2.3.1.2. Opinión de la Presidencia del Consejo de Ministros

Mediante Oficio N° D002111-PCM-SG, de fecha 25 de octubre de 2024, la Presidencia del Consejo de Ministros (PCM), trasladó la opinión institucional de su organismo, la cual, a su vez, contiene la opinión de la Secretaría de Gobierno y Transformación Digital, de la Secretaría de Gestión Pública y de la Oficina General de Asesoría Jurídica de la PCM.

a) Opinión de la Secretaría de Gobierno y Transformación Digital de la PCM

Mediante Informe N° D000001-2024-PCM-SGTD-JPZ, de fecha 22 de octubre de 2024, la Secretaría de Gobierno y Transformación Digital hace suyo y emite opinión técnica con respecto al Proyecto de Ley N° 8842/2024-CR

Al respecto, el análisis señala que el artículo 8 del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, establece que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende la seguridad digital, entre otros ámbitos. También refiere que la propuesta legislativa propone el desarrollo de funciones que actualmente se encuentran atribuidas a la rectoría de la PCM.

En esa misma línea, refiere que mediante el artículo 2 del Decreto Supremo N° 118-2018-PCM, se creó el "Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo", como un órgano de carácter estratégico dependiente de la PCM, cuya finalidad es la coordinación multisectorial, articulación y promoción de las acciones relacionadas al desarrollo y consolidación del gobierno digital, la innovación y la economía digital. Asimismo, indica que el artículo 10 del Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital, señala que el Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo es un espacio de coordinación y articulación entre el sector público, privado, sociedad civil, academia y población para las acciones relacionadas al desarrollo y consolidación de la transformación digital en el país, esto comprende materias de seguridad digital y/o ciberseguridad.

Por otra parte, el artículo 9 de la precitada norma señala que la PCM por medio de la Secretaría de Gobierno y Transformación Digital puede establecer mecanismos de articulación del Sistema Nacional de Transformación Digital para el impulso de sus materias como mesas de diálogo, codiseño o cocreación, comités de expertos, mecanismos de innovación abierta, laboratorios de innovación, equipos público – privados especializados y multidisciplinarios en transformación digital.

El informe recomienda analizar la posibilidad de crear o establecer espacios de diálogo específicos para tratar temas de seguridad digital entre el sector público, privado, sociedad civil, academia y ciudadanos; y proponer el desarrollo de algunas funciones en materia de seguridad digital en la normativa del Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo como mecanismo de coordinación y articulación,

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

concluyendo que el Proyecto de Ley 8842/2024-CR es inviable.

b) Opinión de la Secretaría de Gestión Pública

A través del Informe N° D000449-2024-PCM-SSAP, de fecha 16 de octubre de 2024, la Secretaría de Gestión Pública de la PCM, hace suyo y emite opinión técnica con respecto al Proyecto de Ley N° 8842/2024-CR.

Del análisis, la Secretaría de Gestión Pública de la PCM, advierte que la iniciativa legislativa contiene una propuesta vinculada con una potestad exclusiva del Poder Ejecutivo, como lo es la creación de un órgano colegiado; advierte además que el artículo 23 del Reglamento de la Ley Marco para la Producción y Sistematización Legislativa, aprobado por Decreto Supremo N° 007-2022-JUS, prevé que las disposiciones organizativas "establecen la organización de las entidades, órganos y unidades orgánicas a las cuales se dirigen, precisando las competencias, atribuciones, facultades o funciones que les corresponden", agrega además, que estas disposiciones se rigen por las normas que regulan la estructura, funcionamiento y organización del Estado.

El informe, menciona la Ley N° 29158, Ley Orgánica del Poder Ejecutivo (**LOPE**), norma de desarrollo constitucional, el cual se encuentra sobre la base del artículo 106 de la Constitución, el cual dispone que mediante leyes orgánicas se regulan la estructura y el funcionamiento de las entidades del Estado. Ahora bien, la LOPE regula los órganos colegiados en el ámbito del Poder Ejecutivo, pudiendo tratarse de comisiones, grupos de trabajo, y comités, los que se crean a iniciativa de este Poder del Estado.

En lo referente a la declaración de interés nacional y necesidad pública la creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano refiere que la exposición de motivos de la propuesta legislativa, señala expresamente que resulta necesario la creación de este comité, en tal sentido, la iniciativa legislativa resulta no viable en tanto propone la creación de un órgano colegiado (**comité**), potestad que le corresponde única y exclusivamente al Poder Ejecutivo.

a) Opinión de Oficina General de Asesoría Jurídica de la PCM

Mediante Informe N° D0001559-2024-PCM-OGAJ, de fecha 24 de octubre de 2024, hace suyo y emite opinión técnica en lo referente a la iniciativa legislativa.

En su informe, la Oficina General de Asesoría Jurídica de la PCM, precisa que la propuesta legislativa vulnera el principio de Separación de Poderes y el Principio de Competencia, ya que afecta las competencias y funciones del Poder Ejecutivo, en lo relacionado a la iniciativa para la creación de órganos colegiados, según lo establecido en el artículo 29 de los Lineamientos de Organización del Estado, aprobados mediante Decreto Supremo N° 054-208-PCM.

Del análisis de la iniciativa legislativa, la OGAJ advierte la falta de justificación de la necesidad de propuestas contenidas en la autógrafa de ley, los cuales están reguladas

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

en el artículo 2 de la Ley N° 26889, Ley Marco de la Producción y Sistematización Legislativa, el Manual de Técnica Legislativa del Congreso de la República y en el artículo 75 del Reglamento del Congreso de la República.

Tras el estudio, el informe señala que ni el proyecto de ley ni la exposición de motivos cuentan con justificación para proponer la creación de un Comité de Alto Nivel de Ciberseguridad para la implementación de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, entre otros, por tal sentido, la Oficina General de Asesoría Jurídica de la PCM, concluye que la propuesta legislativa no resulta viable.

2.3.1.3 Opinión del Ministerio de Justicia y Derechos Humanos

Mediante Oficio N° 4882-2024-JUS/SG, de fecha 5 de diciembre de 2024, el Ministerio de Justicia y Derechos Humanos, trasladó la opinión técnica institucional de su organismo, el cual a su vez contiene el Oficio N° 1113-2024-JUS/GA con el Informe Técnico N° 000318-2024-JUS/DGAC de la Dirección General de Asuntos Criminológicos del Ministerio de Justicia y Derechos Humanos.

Respecto a las competencias de la Dirección General de Asuntos Criminológicos, el informe señala que mediante Ley N° 29807, se creó el Consejo Nacional de Política Criminal (CONAPOC), como órgano encargado de planificar, articular, supervisar y dar seguimiento a la política criminal del Estado. En esa línea, de conformidad con el numeral 10 del artículo 4 de su ley de creación, tiene entre sus mandatos y funciones emitir, a través de la Secretaría Técnica, informes técnicos no vinculantes sobre toda propuesta legislativa en materia de justicia penal, ejecución penal y sistema penitenciario con el fin de analizar su grado de adecuación a la Política Criminal.

Que, de conformidad con el artículo 58 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos (ROF del MINJUS), aprobado mediante Decreto Supremo N° 013-2017-JUS, la Dirección General de Asuntos Criminológicos (DGAC) es el órgano de línea encargado de diseñar, formular y evaluar las políticas del Estado en materia criminológica, así como efectuar seguimiento a la ejecución de dichas políticas, proponiendo los correctivos correspondientes; asimismo tiene a su cargo la Secretaría Técnica del CONAPOC.

El informe señala que, de acuerdo a la propuesta legal y exposición de motivos, justifica la propuesta normativa, debido a la necesidad de implementar estrategias, acciones actividades e iniciativas para el desarrollo de la ciberseguridad en el Perú, mediante un órgano de carácter estratégico dependiente de la Presidencia del Consejo de Ministros.

La Dirección General de Asuntos Criminológicos (DGAC) indica que, a pesar de las 12,169 denuncias registradas, entre octubre de 2013 a diciembre de 2020, sobre delitos vinculados a la Ley N° 30096. Ley de Delitos Informáticos, donde el delito de fraude informático posee una incidencia del 78 % (9,515 casos) y el delito de suplantación de identidad una incidencia del 13 %, y los delitos contra datos y sistemas informáticos posee una incidencia del 6 %, solo se han emitido pocas sentencias en el Poder Judicial,

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

en tal sentido, el informe precisa, que surge la necesidad que el Estado atienda la referida problemática expuesta a fin de evitar la impunidad en el sistema de justicia.

Respecto a la seguridad ciudadana, el informe refiere que está relacionada con la Defensa Nacional en el ámbito interno, por cuanto se debe prevenir y asegurar la paz social. El artículo 2 de la Ley N° 27933, Ley del Sistema Nacional de Seguridad Ciudadana, señala que la seguridad ciudadana es la acción multisectorial, integrada y articulada que desarrolla el Estado.

En esa línea, el análisis describe que con el transcurrir del tiempo, se ha podido constatar que el uso de las tecnologías de la información y las comunicaciones (TIC) se ha convertido en parte esencial del quehacer diario de las personas, indistintamente de su edad, estatus social o sus ámbitos de desarrollo social, personal, familiar, educativo, laboral, profesional, comercial, etc.

Durante la etapa de la pandemia, la virtualización en el Perú se hizo más evidente, esto obligó al incremento del uso de las TIC. Sin embargo, el crecimiento del uso de las tecnologías de la información y comunicación ya era una realidad desde la última década. Puesto que, para el año 2010, uno de cada tres peruano usaba internet, mientras que para el 2021 ya lo hacían tres de cada cuatro. Su frecuencia se hizo cada vez mayor y ya para el último trimestre del año 2021, el acceso a internet por parte de los hogares peruanos alcanzó el 55%, esto es, más de 9,6 puntos porcentuales que el mismo periodo 2020.

De manera simultánea las ventajas que generan las TIC trajeron consigo constantes "ciberamenazas" contra la ciudadanía y los Estados, reportándose distintos tipos de ataques y hechos delictivos perpetrados a través de las TIC. Al respecto, la Organización Internacional de Policía Criminal (Interpol), ha comunicado que los ciberdelincuentes han venido evolucionando y cambiando sus objetivos para maximizar los daños y robos. Así, en lugar de lanzar sus ataques contra particulares y pequeñas empresas, han ampliado su espectro, centrando sus delitos en grandes empresas, gobiernos e infraestructuras esenciales.

El Perú no ha sido ajeno al crecimiento global de este fenómeno criminal, pues, tenemos que, de enero a septiembre del año 2021, la Policía Nacional del Perú, recibió un total de 11,985 denuncias de este tipo en todo el país, correspondiendo el 70 % de ellas a la modalidad de fraude informático. De otro lado, desde octubre del 2013 hasta julio del 2020, el Ministerio Público las fiscalías penales comunes y mixtas del Ministerio Público de todo el país registraron 21,687 denuncias por delitos informáticos, clara muestra del aumento considerable de la ciberdelincuencia durante la emergencia sanitaria.

Respecto al rol del Estado, el informe señala que tiene una gran responsabilidad en la prevención y protección contra el cibercrimen, y el deber de garantizar la seguridad de los datos de las personas, por tal motivo, resulta factible la creación de un Comité de Alto Nivel de Ciberseguridad para fortalecer el trabajo multisectorial, establecer alianzas estratégicas con otros países en el ámbito de cooperación internacional, considerando que no se tratan de delitos que se perpetran específicamente en un solo lugar o espacio

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

territorial, sino que, por el contrario, traspasan las fronteras.

En consecuencia, la Dirección General de Asuntos Criminológicos (DGAC) de la PCM, considera que el Proyecto de Ley N° 8842/2024-CR resulta viable.

2.3.1.4 Opinión del Instituto Nacional Penitenciario - INPE

A través del Oficio N° D001293-2024-INPE-PRE, de fecha 3 de diciembre de 2024, el Instituto Nacional Penitenciario (INPE), trasladó la opinión técnica institucional de su organismo, el cual a su vez contiene Memorando N° D001328-2024-INPE-DISEPE con el Informe N° D000072-2024-INPE-DISEPE.ST de la Dirección de Seguridad Penitenciaria – Seguridad Tecnológica.

El informe señala que la creciente dependencia del ciberespacio ha ampliado los escenarios propicios para los ciberdelincuentes, al extremo que en la actualidad constituye uno de los principales riesgos y desafíos en materia de seguridad ciudadana y defensa nacional. Para el Perú, este es un problema que debe generar especial atención por parte del Estado, ya que involucra la afectación de derechos de grupos vulnerables de personas, como niñas, niños, adolescentes y adultos mayores, y de quienes en su mayoría desconocen el manejo y resguardo de datos personales.

Sobre la amenaza del incremento de la ciberdelincuencia, el informe refiere que esta afecta a la seguridad nacional y muestra vulnerable a las instituciones públicas incluido al INPE, razón por la cual, recomiendan que en la iniciativa de ley se integre al INPE como parte del Comité de Alto Nivel de Ciberseguridad del Estado peruano, considerando que cuenta con información privilegiada del sistema penitenciario nacional, además de las herramientas tecnológicas que comprenden diversos programas, aplicativos, software y otros en el desarrollo de sus actividades de administración, seguridad y tratamiento.

Que, el Convenio sobre la Ciberdelincuencia del Consejo de Europa, aprobado y ratificado por el Estado peruano, constituye la norma internacional más completa en esta materia hasta el momento. Promueve la tipificación de los ciberdelitos en las legislaciones penales nacionales, la utilización de herramientas eficaces de derecho procesal que faciliten su detención, investigación y sanción, así como la cooperación internacional rápida y fiable.

En tal sentido, la Dirección de Seguridad Penitenciaria – Seguridad Tecnológica del INPE concluye que el Proyecto de Ley N° 8842/2024-CR "Ley que declara de interés nacional y necesidad pública la creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano" resulta viable.

2.3.2 Proyecto de Ley 9906/2024-CR

Se ha recibido las siguientes respuestas a los pedidos de opinión:

DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY 8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA CREACIÓN DEL COMITÉ DE ALTO NIVEL DE CIBERSEGURIDAD DEL ESTADO PERUANO

Fecha	Institución	Documento
25/02/2025	Cámara de Comercio de Lima	P/232.02.2025/DNPACG
25/02/2025	Ministerio del Interior	Oficio N° 1799-2025-IN-SG
20/03/2025	Presidencia del Consejo de Ministros	Oficio N° D000546-2025-PCM-SG

2.3.2.1 Opinión de la Cámara de Comercio de Lima

Mediante documento P/232.02.2025/DNPACG de fecha 25 de febrero de 2025, la Cámara de Comercio de Lima, trasladó la opinión institucional de su organismo, la cual a su vez contiene el Informe DNPACG-019-2025/CCL de la Dirección de Normatividad, Políticas y Articulación de Comisiones y Gremios.

La Cámara de Comercio de Lima, a través de la Dirección de Normatividad Políticas y Articulación de Comisiones y Gremios, indica que el proyecto de ley tiene por objeto y finalidad materias ya reguladas en la normativa vigente, en esa línea, cita el artículo 8 del Decreto Supremo N° 007-2022-JUS, "Reglamento de la Ley Marco para la Producción y Sistematización Legislativa", el cual señala que toda propuesta normativa debe incluir el análisis respectivo sobre su necesidad en relación al problema público identificado.

En consecuencia, la Cámara de Comercio de Lima, emite opinión desfavorable respecto al Proyecto de Ley N° 9906/2024-CR, Ley de Seguridad Digital o Ciberseguridad.

Oficio N° 634-2024-CG PNP/SEC, de fecha 21 de setiembre de 2024, el secretario de la Comandancia General PNP pone de conocimiento que con Oficio N° 000391-2024-IN-DM de fecha 20 de setiembre de 2024, el ministro del Interior solicitó al presidente del Congreso, que todos los requerimientos dirigidos a la Policía Nacional del Perú, sean dirigidos al Ministerio del Interior.

2.3.2.2 Opinión de la Presidencia del Consejo de Ministros

Mediante Oficio N° D000546-2025-PCM-SG, la Secretaría General de la Presidencia del Consejo de Ministros traslada a esta Comisión la opinión técnica y legal de su entidad.

a) Opinión de la Secretaría de Gobierno y Transformación Digital

Mediante el Memorando N° D000190-2025-PCM-SGTD la Secretaría de Gobierno y Transformación Digital remite el Informe N° D000006-2025-PCM-SSPRD-YAC, a través del cual emite opinión sobre el Proyecto de Ley N° 9906/2024-CR, señalando lo siguiente:

- La SGTD, es el órgano con autoridad técnico-normativa a nivel nacional encargado de proponer, coordinar, implementar y evaluar la Política Nacional de Transformación Digital y su estrategia. Además, supervisa y desarrolla políticas,

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

normas, planes, proyectos y plataformas digitales, y es responsable de la rectoría del Sistema Nacional de Transformación Digital, que involucra al sector público, privado, la sociedad civil, la academia y la ciudadanía en áreas como gobierno, transformación y confianza digital en el país.

- Consistente con el marco legal y el análisis del Proyecto de Ley, notamos lo siguiente: a) El Proyecto de Ley de Seguridad Digital se superpone con las disposiciones establecidas en el Decreto Supremo N° 029-2021-PCM y Decreto de Urgencia N° 007-2020. b) El Proyecto de Ley de Seguridad Digital no reconoce el Marco de Seguridad Digital del Estado Peruano creado en la Ley de Gobierno Digital y su Reglamento. c) El Proyecto de Ley debe referirse a Seguridad Digital en sus disposiciones, dado que es el término usado en el ámbito nacional. Ahora bien, ello no quiere decir que en el desarrollo de medidas técnicas como adopción de estándares o marcos podamos referirlo o promoverlo.
- La SGTD observa el Proyecto de Ley, dado que contraviene todo el Marco de Seguridad Digital creado por el Estado.

b) Opinión de la Secretaría de Gestión Pública

Mediante el Memorando N° D000087-2025-PCM-SGP la Secretaría de Gestión Pública remite el Informe N° D000044-2025-PCM-SSAP, a través del cual emite opinión sobre el Proyecto de Ley N° 9906/2024-CR, señalando lo siguiente:

- Siendo que la propuesta legislativa al pretender crear un órgano colegiado, que, al presidirlo la PCM, debería encontrarse bajo el ámbito del Poder Ejecutivo, le corresponde a dicha entidad evaluar y determinar la pertinencia de su creación. Lo señalado se refuerza con el hecho que corresponde al Ministro proponer la organización interna del Ministerio que se encuentra a su cargo, conforme lo señala el numeral 4 del artículo 25 de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo, con lo cual correspondería a la propia PCM determinar la creación de los órganos colegiados, como son los comités, que se encontrarán bajo su dependencia.
- Sin perjuicio de lo mencionado, cabe precisar que el Comité propuesto en el Proyecto de Ley persigue un objeto que no se alinea a los establecido en los LOE para dicho tipo de colegiado, como por ejemplo el promover una cultura de ciberseguridad, impulsar la incorporación de contenidos sobre ciberseguridad en los currículos de educación superior y de gestionar el Fondo de Seguridad Digital, los cuales constituyen actividades de carácter permanente, con lo cual se desnaturalizaría la razón de ser de dicho tipo de instancias colegiadas en el ámbito del Poder Ejecutivo

c) Opinión de la Oficina General de Asesoría Jurídica de la PCM

De la revisión del Proyecto de Ley N° 9906/2024-CR y conforme a lo señalado por la Secretaría de Gestión Pública, se propone crear un órgano colegiado, Comité de Ciberseguridad, adscrito a la Presidencia del Consejo de Ministros (PCM), lo cual constituye potestad única y exclusiva del Poder Ejecutivo, según lo establecido en

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

el artículo 29 de los Lineamientos de Organización del Estado, aprobado por Decreto Supremo N° 054-2018- PCM.

Asimismo, el numeral 4 del artículo 25 de la Ley N° 29158. Ley Orgánica del Poder Ejecutivo, establece como una de las funciones de los Ministros de Estado, proponer la organización interna de su Ministerio y aprobarla de acuerdo con las competencias que les atribuye esta Ley.

En tal sentido, correspondería a la PCM determinar la creación de órganos colegiados, en este caso, creación de comité, que se encontrará bajo su dependencia, motivo por el cual el Proyecto de Ley bajo análisis vulneraría el Principio de Separación de Poderes, reconocido en el artículo 43 de la Constitución Política del Perú, y el Principio de Competencia, recogido en el numeral VI del Título Preliminar de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo.

En consecuencia, corresponde exclusivamente al Poder Ejecutivo la creación de un órgano colegiado en su ámbito; por lo que, el Proyecto de Ley no resulta viable, toda vez que no se encuentra en concordancia con lo establecido en la Constitución Política del Perú, la Ley N° 29158 y los Lineamientos de Organización del Estado.

2.3.2.3 Opinión del Ministerio del Interior

Mediante Informe N° 000449-2025-IN-OGAJ, elaborado por la Oficina General de Asesoría Jurídica, el Ministerio del Interior emite la opinión solicitada, la misma que contiene las opiniones de las siguientes:

a) Opinión del Despacho Viceministerial de Seguridad Ciudadana

El Despacho Viceministerial de Seguridad Ciudadana analiza el impacto del proyecto en la seguridad pública y enfatiza la necesidad de una implementación coordinada con los distintos niveles de gobierno y fuerzas del orden. En su evaluación, destaca la importancia de establecer estrategias operativas que permitan una ejecución efectiva sin afectar los recursos destinados a la lucha contra la criminalidad. Asimismo, subraya la necesidad de fortalecer los mecanismos de supervisión y control con el propósito de prevenir posibles vulneraciones al marco normativo vigente. Finalmente, recomienda ajustes en la propuesta con el objetivo de optimizar su operatividad y asegurar su alineación con la política nacional de seguridad ciudadana.

b) Opinión del Despacho Viceministerial de Orden Interno

El Despacho Viceministerial de Orden Interno examina la viabilidad del proyecto en relación con el mantenimiento del orden público y la prevención de conflictos sociales. En su análisis, resalta la importancia de que cualquier modificación normativa no afecte las competencias ni las atribuciones de los organismos responsables de la seguridad y el control del orden. Asimismo, identifica la necesidad de una mayor precisión en la redacción del proyecto con el fin de evitar

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

ambigüedades que puedan generar conflictos de interpretación en su aplicación. Adicionalmente, enfatiza la relevancia de articular la propuesta con otras disposiciones legales en materia de seguridad interna para garantizar su coherencia normativa y operativa.

c) Opinión de la Policía Nacional del Perú

La Policía Nacional del Perú (PNP) emite su opinión técnica respecto a la aplicabilidad del proyecto y sus implicancias en el desempeño operativo de la institución. En su evaluación, señala posibles impactos en el despliegue de efectivos policiales y en la administración de recursos logísticos necesarios para su implementación. La PNP advierte sobre la importancia de reforzar los mecanismos de capacitación y los lineamientos de actuación para el personal policial con el fin de garantizar una ejecución eficiente y alineada con los protocolos institucionales. Asimismo, propone la inclusión de disposiciones que permitan una adecuada supervisión y evaluación de los resultados, con el objetivo de realizar ajustes en su implementación en caso de ser necesario.

d) Opinión Legal de la Oficina General de Asesoría Jurídica

La Oficina General de Asesoría Jurídica realiza un análisis de compatibilidad normativa del proyecto con el marco legal vigente. En su informe, identifica posibles riesgos jurídicos derivados de su implementación y señala aspectos que requieren ajustes con el propósito de evitar conflictos normativos o vacíos legales. Concluye que, si bien la propuesta es jurídicamente viable, resulta necesario precisar ciertos términos y delimitar con mayor claridad las competencias de los actores involucrados. Asimismo, recomienda llevar a cabo una revisión exhaustiva de la propuesta para asegurar su coherencia con otras disposiciones legales y prevenir futuras controversias en su aplicación.

III. MARCO NORMATIVO

El análisis realizado se basa en el siguiente marco normativo, relacionados con el desarrollo de la ciencia, la tecnología y la innovación.

- Constitución Política del Perú.
- Reglamento del Congreso.
- Ley N° 30999. Ley de la Ciberdefensa.
- Ley N° 27309, Ley que incorpora los delitos informáticos al Código Penal.
- Ley N° 30096, Ley de Delitos Informáticos.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Decreto Supremo N° 012-2017-DE, Decreto Supremos que aprueba la Política de Seguridad y Defensa Nacional.
- Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo 050-2018-PCM, Decreto Supremo que establece la definición de Seguridad Digital en el ámbito nacional.

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

- Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto Supremo N° 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema de Transformación Digital.
- Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento de la Ley de Gobierno Digital.

IV. ANÁLISIS DE LAS PROPUESTAS LEGISLATIVAS

El Proyecto de Ley 8842/2024-CR propone declarar de interés nacional y necesidad pública la creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano, toda vez que resulta necesario que el Perú implemente una política, ley o estrategia relacionada a la ciberseguridad para garantizar la seguridad informática y protección de datos en todo el territorio patrio, facilitando la identificación, evaluación y gestión de riesgos cibernéticos a un nivel que involucra todos los aspectos de una organización.

La iniciativa de ley tiene como propósito adoptar medidas concretas ante el avance de la criminalidad cibernética, el cual evoluciona de la mano de la tecnología, haciendo que la amenaza cibernética ponga en serio riesgo la seguridad nacional, financiera y social del Perú, como consecuencia de la falta de políticas, herramientas y estrategias que permitan una lucha frontal a este delito que va ganando terreno y garantice la protección de datos activos y sensibles.

Respecto al Proyecto de Ley 9906/2024-CR, Ley de Seguridad Digital o Ciberseguridad, esta tiene por objeto establecer el marco normativo de la seguridad digital en el Estado peruano, con el objetivo de proteger la información digital, dispositivos, activos, incluidos la información personal, cuentas del sistema financiero, archivos, imágenes y el patrimonio del Estado, así como de las personas naturales y jurídicas frente a los ciberataques que se incrementan de manera alarmante en el país.

4.1 Marco Conceptual: Ciberseguridad

Existe una amplia variedad de definiciones respecto a que es la Ciberseguridad, sin embargo, todas apuntan al mismo propósito, en consecuencia, se consideró la siguiente:

*"Se define a la ciberseguridad como la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados"*¹.

Para entender mejor la definición de Ciberseguridad, es necesario conocer la definición

¹Isaca (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información).

DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO

de **Activo de la Información**, el cual de acuerdo a la Norma ISO 27001 de estándar internacional que establece los requisitos para gestionar la seguridad de la información, son los conocimientos o datos que tienen valor para una determinada organización, en esa misma línea la norma define a los **Sistemas de Información** como aquellas aplicaciones, servicios, activos de tecnologías de información u otros que permiten el manejo de la misma².

En consecuencia, se puede afirmar que la ciberseguridad, tiene como objetivo principal la protección de la información digital que almacenan los sistemas interconectados y están comprendidos dentro de la seguridad de la información.

Según la Real Academia Española (RAE), la seguridad se define como: Libre o exento de todo peligro, daño o riesgo³. Sin embargo, esta es una condición ideal que no alcanza a la realidad, pues es innegable que se puedan evitar todos los peligros. En consecuencia, el propósito de la seguridad en todos sus ámbitos, incluido la ciberseguridad, es el de reducir riesgos hasta un nivel que se pueda aceptar y mitigar las amenazas latentes. Es decir que la seguridad que las actividades se encuentran destinadas a proteger del peligro a los activos sensibles de la organización⁴.

La era digital en la que vive el Perú avanza a pasos agigantados, donde el uso de las tecnologías de la información y comunicaciones se ha vuelto indispensable para toda actividad profesional, personal o familiar. De manera simultánea este avance trae consigo el acrecentamiento de medios tecnológicos con fines delictivos.

El incremento de ataques cibernéticos y continua vulneración de los sistemas de información, ponen de manifiesto la necesidad de adoptar medidas, políticas, estrategias y controles que permitan proteger al Estado ante estas amenazas que van ganando terreno en la lucha contra la cibercriminalidad.

La capacidad delincuencia en el ciberespacio se incrementado de manera considerable, junto a ella, el uso de nuevas tecnologías genera una amenaza y preocupación constante para todos los países, dado que impactan de manera directa a los órganos públicos y privados, así como las personas naturales.

Trabajar temas de ciberseguridad implica un serio compromiso del Gobierno nacional, pues se debe garantizar la seguridad de la información para tranquilidad de la sociedad. En relación a este tema, varios países han implementado políticas y estrategias en ciberseguridad nacional, considerando su importancia como documento estratégico que sirve como fundamento para desarrollar las previsiones de la estrategia de seguridad

²Norma ISO/IEC 27001:2022

³Real Academia Española y Asociación de Academias de la Lengua Española: Libro de estilo de la lengua española [en línea]. <https://www.rae.es/libro-estilo-lengua-espanola/citas>

⁴GAVINO RAMOS, Martín (2018). Ciberseguridad en la actividad organizacional de la era digital. Universidad Nacional Federico Villareal; Lima. Recuperado de https://web.unfv.edu.pe/facultades/fiis/images/oficinas/unidad_investigacion/INVESTIGACION_2019/MIERCOLES8/FIIS_IF2018_GAVINO_RAMOS_MARTIN.pdf

DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO

nacional en materia de protección del ciberespacio con el fin de establecer de forma coherente y estructurada acciones de prevención, defensa, detención y respuesta ante la ciberdelincuencia.

Por ello, resulta necesario que las autoridades adopten medidas que proporcionen un tratamiento adecuado y efectivo en la prevención de daños e impunidad en la lucha contra la cibercriminalidad. Toda vez que en el Perú se registra un alto índice porcentual de delitos cibernéticos, además de la falta de capacidad de respuesta de los órganos encargados de investigar y regular este fenómeno delictivo.

4.1.1 Ciberseguridad en otros países de la región

- a) **Chile.** - En el país sureño, existe la "Alianza Chile de Ciberseguridad", fundada por nueve (9) instituciones que representan a sectores importantes del país integrados por organismos estatales, privados y académicos. Esta alianza tiene por objetivo cooperar con las autoridades en esta materia (ciberseguridad), generando nuevas redes de contacto y alianzas internacionales.

Para Michelle Bachelet, expresidenta de la República de Chile, define a la ciberseguridad como una política que debe estar acompañada de las tecnologías de la información y la comunicación (TIC), como una herramienta indispensable sin comparación en la historia que las personas, para las interacciones institucionales, los trámites, las operaciones y las comunicaciones privadas y públicas.

Las TIC en Chile han tenido un impacto social sin precedentes, permitiendo entre otras acciones, que los ciudadanos se mantengan informados y se organicen mediante las redes digitales, otorgándoles principalmente a los niños y adolescentes espacios de interactividad y aprendizaje.

Chile trabajó sus políticas de ciberseguridad, con el claro objetivo y lineamientos de brindarle a los chilenos espacios libres, abiertos y seguros, sobre todo por la necesidad de contar con políticas de gestión y minimización de riesgos y amenazas, principalmente en lo relacionado a infraestructuras críticas de la información, considerando reglas especiales para la adquisición y operación de soluciones tecnológicas que toman en cuenta el contexto internacional existente en materia de ciberseguridad.

El Decreto Supremo N° 533/2015-Chile, tiene como objetivo primordial definir una política nacional de ciberseguridad y órgano asesor de Gobierno.

- b) **Colombia.** - Fue uno de los primeros en adoptar una Estrategia Integral de Ciberseguridad cuyos vectores de desarrollo sobre materia de ciberseguridad para Colombia, están orientadas a fortalecer la posición del país⁵, alineados con las diferentes estrategias nacionales provenientes desde las entidades del Estado y del

⁵LEIVA, Alfredo (2015). "Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una visión global a una visión local". Revista Latinoamericana de Ingeniería de Software, 3(4), p. 161-176.

⁶INTERNATIONAL TELECOMMUNICATION UNION (2024). Global Cybersecurity Index. 5th Edition. ITU Publications.

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

sector privado y, que con su fortalecimiento conlleven a mejorar la posición estratégica del país en estos temas.

Colombia ha empezado a plantear una visión rectora consolidada en el documento CONPES 3701, el cual busca generar los lineamientos nacionales de política en Ciberseguridad orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.

En este marco de referencia se define la Ciberseguridad como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Como antecedentes normativos, se muestra la Ley 527 de 1999, el cual define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y establece las entidades de certificación y se dicta además otras disposiciones.

Uno de los trabajos más recientes es el Decreto 338 del año 2022, por medio del cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de estructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital⁶.

Sin embargo, uno de los trabajos que se muestra como la columna vertebral en temas de ciberseguridad en Colombia, es la que se realizó en Bogotá en 2014, y es la Agenda Estratégica de Innovación y Ciberseguridad, elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones de la República de Colombia, el cual abarca vectores de desarrollo claramente identificables:

- Principios rectores de ciberseguridad.
- Educación, formación y divulgación de ciberseguridad.
- Gestión integrada de riesgos e incidentes de la naturaleza cibernética.
- Identificación, autenticación y autorización.
- Aseguramiento de aplicaciones y ambientes móviles en el gobierno.
- Tecnologías de la información y las comunicaciones para el sector Defensa.

- c) **Brasil.** - Es el país de América Latina que presenta la mayor madurez en ciberseguridad. Pasa a segundo lugar cuando la medición se traslada a toda América y solo es superada por Estados Unidos. En materia de ciberseguridad, Brasil, mostró una evolución considerable en los últimos seis años, al pasar del sexto lugar en el continente, al tercero en 2021, resultado que pone en vitrina mundial el trabajo que viene desarrollando este país en la materia.

En la última publicación del Índice Global de Ciberseguridad 2024 (IGC 2024) realizado por la Unión Internacional de Telecomunicaciones (UIT)⁶, que evalúa cinco criterios objetivos para calificar a los países: marco normativo, acciones técnicas,

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

iniciativas organizativas, desarrollo de capacidades y actividades cooperativas. De estas variables dependen las calificaciones finales donde T1 es ejemplar, T2 es avanzado, T3 representa un nivel estable, T4 significa evolución y T5 en construcción. Brasil, obtuvo calificación T1, la más alta, al igual que otros 45 países del mundo (en su mayoría de Europa, Asia Pacífico, los estados árabes y África). Fue además el único en América latina en lograrla.

Su marco legal y las acciones técnicas y cooperativas fueron donde obtuvo las mejores notas, seguidas por su capacidad de desarrollo y su acción organizativa.

Este avance significativo en materia de ciberseguridad, tiene su génesis en el papel que tomó Brasil desde el año 1995, cuando notó que el desarrollo del internet requería gobernanza. En ese marco, en mayo de 1995 creó el Comité Gestor de Internet de Brasil, propuesta por el entonces Ministerio de Comunicación y el Ministerio de Ciencia y Tecnología (actualmente Ministerio de Ciencia, Tecnología Innovación y Comunicación), este comité impulsó el multisectorialismo en su gobernanza, además de abordar las cuestiones de seguridad.

4.1.2 Resultados Índice Global de Ciberseguridad 2024 (IGC 2024)

a) Resultados América Latina y El Caribe

La quinta edición del Índice Global de Ciberseguridad (IGC) mide los compromisos de los países con la ciberseguridad según el contexto de medidas en estos cinco pilares: legal, técnico, organizativo, desarrollo de capacidades y cooperación⁷.

Los países de América Latina y El Caribe destacan en diferentes aspectos de la evaluación, reflejando enfoques específicos y capacidades en el fortalecimiento de su ciberseguridad.

- **Liderazgo regional:** Brasil, Uruguay y Ecuador ocupan los tres primeros lugares en la región, gracias a sus esfuerzos integrales en legislación, capacidades técnicas y cooperación internacional en ciberseguridad.
- **Aspecto legal:** Perú, Brasil y Cuba obtienen la puntuación máxima de 20 puntos en este indicador, lo que evidencia un marco legislativo sólido y actualizado.
- **Aspecto técnico:** Brasil y Uruguay lideran con 20 puntos, destacando por su capacidad técnica avanzada, incluyendo equipos de respuesta ante incidentes (CIRTs) y tecnología para la gestión de riesgos cibernéticos.

⁷RESULTADOS ÍNDICE GLOBAL DE CIBERSEGURIDAD 2024. Recuperado de <https://cdn.www.gob.pe/uploads/document/file/7365377/6283830-reporte-del-indice-global-de-ciberseguridad-2024%282%29.pdf>

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
 8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
 DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
 CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
 CIBERSEGURIDAD DEL ESTADO PERUANO**

- Aspecto organizacional:** Uruguay, El Salvador y Ecuador sobresalen con puntuaciones cercanas a los 20 puntos, reflejando estructuras organizativas robustas, como estrategias nacionales de ciberseguridad y organismos dedicados a su implementación.
- Desarrollo de capacidades:** Uruguay y Brasil lideran con puntuaciones cercanas a los 20 puntos, gracias a inversiones en educación, formación y creación de talento en ciberseguridad, preparando a sus ciudadanos y profesionales para enfrentar desafíos digitales.
- Cooperación:** Brasil es el único país que alcanza la puntuación máxima de 20 puntos, demostrando un liderazgo significativo en colaboración internacional. Panamá y Ecuador le siguen de cerca, con puntuaciones alrededor de los 18 puntos.

b) Resultados Perú

En la medición IGC 2024, Perú alcanzó el puesto 5 de 33 países de América Latina y El Caribe, por encima de países como Chile, Argentina y Costa Rica.

A nivel global, Perú fue clasificado en el Nivel 3 – “Nivel Estable” junto con países como Chile, Colombia y Costa Rica. Dicha clasificación representa a los países que obtuvieron una clasificación general de al menos 55/100 al demostrar un compromiso básico de ciberseguridad con acciones impulsadas que abarcan la evaluación, el establecimiento o la implementación de ciertas medidas de ciberseguridad generalmente aceptadas en un número moderado de pilares o indicadores

Cuadro N° 01: Medición IGC 2024



**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
 8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
 DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
 CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
 CIBERSEGURIDAD DEL ESTADO PERUANO**

Fuente: IGC 2024⁸

Al comparar los resultados de la edición 2024, con los de la edición anterior de 2020, se evidencia una mejora en todos los criterios evaluados.

Cuadro N° 02: Cuadro comparativo de resultados IGC 2020 - 2024

CRITERIO	2024		2020		Variación en puntos 2024 - 2020	Variación en posición 2024 - 2020
	Puntos	Posición regional	Puntos	Posición regional		
Legal	20	2	20	2	0 ●	0
Técnico	13.51	10	11.58	7	+ 1.93 ●	↘ - 3
Organizacional	18.27	5	5.63	15	+ 12.64 ●	↗ +10
Desarrollo de capacidades	15.16	5	5.32	14	+ 9.84 ●	↗ +9
Cooperación	16.8	4	13.15	6	+ 3.65 ●	↗ +2

⁸RESULTADOS ÍNDICE GLOBAL DE CIBERSEGURIDAD 2024.

Fuente: PCM – SECRETARÍA DE GOBIERNO Y TRANSFORMACIÓN DIGITAL⁹

De los resultados, se puede concluir que Perú refleja un compromiso creciente con la ciberseguridad. Los logros alcanzados en el área de desarrollo de capacidades, donde incrementó sus puntos en relación con la edición del 2020, evidencian una mejor formación en el ámbito cibernético. Además, ha incrementado su cooperación internacional, manteniendo también una legislación estable que, junto con medidas de protección de datos personales, refuerza la infraestructura cibernética nacional.

Sin embargo, a pesar de lo avanzado, aún existen brechas que tienen que cerrarse en temas de ciberseguridad, pues el Perú ha experimentado una caída en el criterio “Técnico” donde se descendió tres posiciones desde 2020. Esto señala deficiencias en la implementación de medidas técnicas de defensa cibernética, pues, aunque existen políticas básicas de ciberseguridad, la implementación efectiva de medidas avanzadas y la capacidad de respuesta ante incidentes aún son limitadas.

En consecuencia, para que el Perú alcance al Nivel 2 (T2) es decir “Nivel Avanzado”, necesita implementar áreas clave como infraestructura técnica y la cooperación pública-privada, así como el incremento de inversión en tecnologías de protección, monitoreo de amenazas y respuesta a incidentes, áreas en las que países de Nivel 2, como Brasil y Estados Unidos han demostrado avances significativos¹⁰.

⁸RESULTADOS ÍNDICE GLOBAL DE CIBERSEGURIDAD 2024.

⁹PCM-SECRETARÍA DE GOBIERNO Y TRANSFORMACIÓN DIGITAL.
<https://cdn.www.gob.pe/uploads/document/file/7365377/6283830-reporte-del-indice-global-de-ciberseguridad-2024%282%29.pdf>

¹⁰PCM – SECRETARÍA DE GOBIERNO Y TRANSFORMACIÓN DIGITAL. Recuperado de

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

4.1.3. Convenio de Budapest

Es el "Convenio sobre la Ciberdelincuencia" y está vigente desde diciembre de 2019, el cual es un instrumento jurídico que permite a los jueces y fiscales realizar requerimientos de cooperación internacional vinculados a delitos informáticos, los que de acuerdo con la legislación peruana se encuentran regulados en la Ley N° 30096, modificada por la Ley N° 30171.

Este convenio es un mecanismo de cooperación entre los Estados miembros del Consejo de Europa y las demás economías firmantes, que tiene como finalidad proteger a la sociedad frente a la "ciberdelincuencia", principalmente mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional.

La incorporación de Perú al Convenio de Budapest constituye un notable avance hacia el desarrollo de una economía digital donde se promueva el bienestar social, la productividad territorial, la competitividad y el desarrollo económico en un ambiente de confianza digital entre el sector público, privado y la sociedad.

Dentro del Convenio sobre la Ciberdelincuencia, se resalta aspectos importantes, el cual engloba la necesidad de aplicar con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, ya que el riesgo de que las redes informáticas y la información electrónica sean utilizados igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes¹¹.

4.1.4. Importancia de la Ciberseguridad

Como lo sostiene José Luís Gamboa Suárez, de la Universidad Piloto de Colombia, "Durante los últimos años el auge en los crímenes digitales o ciberataques ha puesto en jaque a los usuarios de internet, sitios web, empresas y corporaciones, generando pérdidas de miles de millones de dólares al año con tendencia al alza debido a que cada día los cibercriminales mejoran o evolucionan sus métodos para lograr acceder a la información personal y confidencial de las víctimas y con ello obtener un lucro económico"¹².

Debido a estas amenazas, es importante la implementación de políticas y herramientas en ciberseguridad, ya que para combatir sus amenazas se debe de contar con conocimientos mínimos de como contrarrestarlas y no ser víctimas de la vulneración de datos informáticos que conlleven al robo de información, fraudes o estafas. Por esos motivos, es que la seguridad informática o ciberseguridad toma tanta relevancia, no solo desde el punto de vista de resguardo de información, sino también económico.

<https://cdn.www.gob.pe/uploads/document/file/7365377/6283830-reporte-del-indice-global-de-ciberseguridad-2024%282%29.pdf>

¹¹CONVENIO SOBRE LA CIBERDELINCUENCIA. Recuperado de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

¹²GAMBOA, José. (2020). Importancia de la seguridad informática y ciberseguridad en el mundo actual. Universidad Piloto de Colombia.

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

4.1.5 La Ciberseguridad en el Perú

En 2020 el BID realizó un informe sobre ciberseguridad en América Latina y El Caribe, destacando aspectos de avances y retrocesos respecto al informe de 2016. En lo que refiere al Perú, el informe precisa que si bien aún no se cuenta con una estrategia nacional de seguridad cibernética, sí se ha puesto en marcha una política nacional de ciberseguridad que, entre otras cosas, destaca la necesidad de crear una estrategia nacional de ciberseguridad y un Comité Nacional de Ciberseguridad¹³.

El informe indica que Perú cuenta con un Equipo de Respuesta ante Incidentes de Seguridad Digital (CSIRT) nacional, cuya misión es coordinar la prevención, el tratamiento y la respuesta de incidentes de seguridad cibernética de instituciones del sector público, así como elaborar estrategias, prácticas y mecanismos necesarios para satisfacer las necesidades de seguridad de la información del Estado.

En junio de 2018, el Gobierno peruano llevó adelante la Conferencia Internacional "Desafíos y Gestión en Seguridad Digital", organizada por la Dirección Nacional de Inteligencia y la Secretaría de Gobierno Digital.

El tema de gobierno digital es importante, por ello se aprobó la Ley de Gobierno Digital, la cual tiene como objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno.

Con respecto a la legislación, Perú cuenta con la Ley N° 30096, "Ley de Delitos Informáticos", que brinda disposiciones sustantivas sobre dicho tipo de delito y, la Ley N° 27309. Que incorporó el delito informático al Código Penal. Por último, cabe mencionar la Ley 29733 sobre la protección de datos personales, que se aplica tanto a bases de datos públicas como privadas.

V. ANÁLISIS COSTO BENEFICIO

El análisis costo-beneficio de los Proyectos de Ley 8842/2024-CR y 9906/2024-CR, debe considerar no solo viabilidad económica y presupuestaria, sino también los beneficios que estas proporcionarían en términos de seguridad, protección de datos, prevención de daños y el ordenamiento administrativo, haciéndolo más idóneo, necesario y ponderado respecto a la Ciberseguridad o seguridad informática.

En consecuencia, la implementación de la iniciativa legislativa que acumula ambos

¹³ REPORTE CIBERSEGURIDAD (2020). Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y El Caribe. Bid.-OEA.

**DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO**

proyectos de ley, no implica una carga financiera significativa para el Estado, toda vez que su principal objetivo es regular la seguridad en el uso de herramientas tecnológicas y fomentar la creación de dependencias especializadas como el Comité de Alto Nivel de Ciberseguridad, cuya integración estará conformada por profesionales del sector público y especialistas del sector privado trabajando en un enfoque colaborativo

Desde el punto de vista económico, la implementación y mantenimiento de infraestructura tecnológica generaría costos en la compra o desarrollo de sistemas de protección, así como para su mantenimiento y actualizaciones. Toda vez que serán necesarias acceder a tecnologías avanzadas de protección de datos, sistemas de detección de intrusos y software de encriptación, mientras que las herramientas tecnológicas requieren mantenimiento y actualización constante.

En términos de beneficio, se podrá prevenir ciberataques que podrían afectar gravemente a sectores importantes del Estado e instituciones privadas, reduciendo la vulnerabilidad del sistema digital y de datos informáticos de instituciones y ciudadanos, generando confianza en la población y permitiendo cumplir los estándares internacionales respecto a la protección de datos.

Además, las pérdidas económicas debido a ciberataques se reducirán considerablemente, ya que el fraude o secuestro de datos generan pérdidas millonarias para los sectores público y privado, en consecuencia, se fortalecerá la estabilidad del mercado, mejorando la competitividad y fomentando el desarrollo de nuevas tecnologías y servicios digitales.

VI. RELACIÓN CON EL ACUERDO NACIONAL Y POLÍTICAS DE ESTADO

Los presentes proyectos de ley concuerdan con el Acuerdo Nacional a través de las siguientes políticas de Estado:

Políticas de Estado 24: Afirmación de un Estado eficiente y transparente

"Nos comprometemos a construir y mantener un Estado eficiente, eficaz, moderno y transparente al servicio de las personas y de sus derechos, y que promueva el desarrollo y buen funcionamiento del mercado y de los servicios públicos. (...) Garantizaremos una adecuada representación y defensa de los usuarios de estos servicios, la protección a los consumidores y la autonomía de los organismos reguladores".

Políticas de Estado 28: Plena vigencia de la Constitución y de los derechos humanos y acceso a la justicia e independencia judicial

"Nos comprometemos a garantizar el acceso universal a la justicia, la promoción de la justicia de paz y la autonomía, independencia y el presupuesto del Poder Judicial así como regular la complementariedad entre éste y la justicia comunal. Asimismo, nos comprometemos a adoptar políticas que garanticen el goce y la vigencia de los derechos fundamentales establecidos en la Constitución y en los

DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO

tratados internacionales sobre la materia".

Políticas de Estado 35: Sociedad de la información y sociedad del conocimiento

"Promoveremos el acceso universal al conocimiento a través de las Tecnologías de la Información y Comunicación (TIC), acompañado de la generación de contenidos, servicios y bienes digitales, así como del desarrollo de capacidades para que todos los peruanos puedan desempeñarse plenamente y de manera segura en el entorno digital, y de igual manera promoveremos mecanismos que fortalezcan el acceso, conectividad y su uso en las regiones del país".

VII. CONCLUSIÓN

Por las consideraciones expuestas, la Comisión de Ciencia, Innovación y Tecnología, de conformidad con el inciso b) del artículo 70 del Reglamento del Congreso de la República, recomienda la **APROBACIÓN** de los Proyectos de **Ley 8842/2024-CR y 9906/2024-CR**, proponiendo un **TEXTO SUSTITUTORIO** en los siguientes términos:

TEXTO SUSTITUTORIO

EL CONGRESO DE LA REPÚBLICA:

Ha dado la Ley siguiente:

**LEY QUE DECLARA DE INTERÉS NACIONAL LA CREACIÓN DEL COMITÉ DE
ALTO NIVEL DE CIBERSEGURIDAD DEL ESTADO PERUANO**

Artículo único. Declaratoria de interés nacional

Se declara de interés nacional la creación del Comité de Alto Nivel de Ciberseguridad del Estado Peruano, a fin de implementar herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los datos activos de una organización y de los usuarios de un ciber entorno.

Dese cuenta.
Sala de Comisiones.
Lima, marzo de 2025.



Firmado digitalmente por:
PARIONA SINCHE Alfredo
FAU 20181749128 soft
Motivo: Soy el autor del
documento
Fecha: 08/04/2025 16:25:38-0500

ALFREDO PARIONA SINCHE

Presidente

Comisión de Ciencia, Innovación y Tecnología

DICTAMEN RECAIDO EN LOS PROYECTOS DE LEY
8842/2024-CR Y 9906/2024-CR, LEY QUE DECLARA
DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA
CREACIÓN DEL COMITÉ DE ALTO NIVEL DE
CIBERSEGURIDAD DEL ESTADO PERUANO



Firmado digitalmente por:
ZEBALLOS MADARIAGA Carlos
Javier FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 09/04/2025 14:35:18-0500



Firmado digitalmente por:
MALAGATRILLO George
Edward FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 09/04/2025 11:18:54-0500



Firmado digitalmente por:
MALAGATRILLO George
Edward FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 09/04/2025 11:18:27-0500



Firmado digitalmente por:
ACUÑA PERALTA Segundo
Hector FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 09/04/2025 15:45:10-0500



Firmado digitalmente por:
ALVAROJAS Carlos Enrique
FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 09/04/2025 15:59:53-0500



Firmado digitalmente por:
BUSTAMANTE DONAYRE Carlos
Ernesto FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 10/04/2025 08:37:09-0500



Firmado digitalmente por:
CICCIA VASQUEZ Miguel
Angel FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 11/04/2025 14:23:20-0500



Firmado digitalmente por:
JIMENEZ HEREDIA David
Julio FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 14/04/2025 12:59:10-0500



Firmado digitalmente por:
FLORES RUIZ Victor
Seferino FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 11/04/2025 18:09:52-0500



Firmado digitalmente por:
MONTEZA FACHO Silvia
Maria FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 14/04/2025 14:52:54-0500



Firmado digitalmente por:
SANTISTEBAN SUCLUPE
Magally FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 14/04/2025 17:22:58-0500



Firmado digitalmente por:
CERRON ROJAS Waldemar
Jose FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 14/04/2025 12:10:20-0500



Firmado digitalmente por:
PAREDES FONSECA Karol
Ivett FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 14/04/2025 16:47:15-0500