Proyecto de Ley N° 9906/2024-CR

WILSON SOTO PALACIOS
CONGRESISTA DE LA REPÚBLICA

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año de la recuperación y consolidación de la economía peruana"

CONGRESO DE LA REPÚBLICA
Área de Trámite Documentario
13 ENE. 2025
RECIBIDO
Firma: Hora: 2:55 p.m.

LEY DE SEGURIDAD DIGITAL O CIBERSEGURIDAD

El Congresista de la República que suscribe, **Wilson Soto Palacios** y los Congresistas integrantes del **Grupo Parlamentario Acción Popular**, y demás Congresistas firmantes, al amparo de lo dispuesto en el artículo 107 de la Constitución Política del Perú y conforme los artículos 22° inciso c), 75° y 76 del Reglamento del Congreso de la República, presentan la siguiente iniciativa legislativa:

FÓRMULA LEGAL.

LEY DE SEGURIDAD DIGITAL O CIBERSEGURIDAD

EL CONGRESO DE LA REPÚBLICA
Ha dado la Ley siguiente:

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto de la Ley

La presente ley tiene por objeto establecer el marco normativo de la 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

wsoto@congreso.gob.pe
www.congreso.gob.pe

Edificio Fernando Belaúnde Terry - Jirón Huallaga N° 368, Oficina 302 – Lima
Central Telefónica: 311-7777 Anexo: 7218

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 incidentes de ciberseguridad

Los mecanismos de comunicación de incidentes entre la sociedad civil, el sector privado, la academia, la comunidad técnica y el sector gubernamental deberán garantizar la confidencialidad de los casos que puedan afectar a 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.

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

CAPITULO 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 manera 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 la 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.

CAPITULO II
CIBERSEGURIDAD EN EL SECTOR PRIVADO

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

El Comité Ad honorem de Ciberseguridad del Estado Peruano establecerá los lineamientos necesarios para la creación y operación de equipos de respuesta frente 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 y privadas, así como las instituciones académicas, la sociedad civil y la comunidad técnica, deberán establecer sus acciones en el principio de cooperación mutua para garantizar el mantenimiento y fortalecimiento de la ciberseguridad a nivel nacional.

DISPOSICIONES COMPLEMENTARIAS FINALES

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*.

DISPOSICION COMPLEMETARIA FINAL

ÚNICA. Vigencia

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

Lima, enero 2025

FIRMA DIGITAL
Firmado digitalmente por: VERGARA MENDOZA Elvis Heman FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 10/01/2025 14:07:44-0500

CONGRESO de la REPÚBLICA
Firmado digitalmente por: SOTO PALACIOS Wilson FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 09/01/2025 16:10:04-0500

FIRMA DIGITAL
Firmado digitalmente por: DOROTEO CARBAJO Raul Felipe FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 10/01/2025 15:55:23-0500

FIRMA DIGITAL
Firmado digitalmente por: VERGARA MENDOZA Elvis Heman FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 10/01/2025 14:08:01-0500

FIRMA DIGITAL
Firmado digitalmente por: MONTEZA FACHO Silvia Maria FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 10/01/2025 15:30:29-0500

FIRMA DIGITAL
Firmado digitalmente por: MORI CELIS Juan Carlos FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 10/01/2025 15:48:36-0500

CONGRESO de la REPÚBLICA
Firmado digitalmente por: ARAGON CARREÑO Luis Angel FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 13/01/2025 10:24:53-0500

I. EXPOSICIÓN DE MOTIVOS

En el contexto actual, las herramientas tecnológicas han transformado radicalmente la manera en que las personas, empresas y gobiernos gestionan la información. Estas herramientas trascienden fronteras geográficas, permitiendo que, desde cualquier parte del mundo, se acceda a sistemas interconectados que operan en computadoras y redes de comunicación al servicio del Estado, así como de personas naturales y jurídicas, tanto de derecho público como privado. En la actualidad, resulta impensable concebir un país u organización que no dependa, en alguna medida, de sistemas informáticos para su desarrollo económico, social y administrativo (Organización de Estados Americanos [OEA], 2020)[1].

Sin embargo, el creciente uso de estas tecnologías conlleva riesgos significativos. Los sistemas informáticos almacenan información sensible que, si es mal utilizada o accedida sin autorización, puede causar graves daños al patrimonio, la privacidad y la seguridad de individuos, organizaciones y de la sociedad en general. Este escenario subraya la necesidad de implementar medidas robustas de protección y fomentar un trabajo coordinado que involucre a todos los actores, tanto públicos como privados, relacionados con la ciberseguridad (Unión Internacional de Telecomunicaciones [UIT], 2020)[2].

El Estado administra información personal altamente sensible sobre sus ciudadanos, incluyendo datos educativos, médicos, financieros y profesionales. Asimismo, gestiona información estratégica relacionada con la seguridad interna y externa, la capacidad económica, recursos armamentistas y la protección de dignatarios y funcionarios de alto nivel, tanto nacionales como extranjeros. Por otro lado, las empresas privadas poseen información digital de alta confidencialidad, crítica para su operación y desarrollo, así como datos de sus clientes que, en caso de ser vulnerados, podrían ocasionar severos daños económicos y de reputación (Gobierno del Perú, 2017)[3].

La ciberseguridad, definida como la práctica de proteger información digital, dispositivos y activos frente a ciberataques, se erige como una necesidad estratégica. Su objetivo principal es

[1] *Unión Internacional de Telecomunicaciones (UIT). (2020). Informe sobre Ciberseguridad Global. Ginebra: UIT.*
[2] *Ídem.*
[3] *Gobierno del Perú. (2017). Estrategia Nacional de Ciberseguridad 2017-2021. Lima: Ministerio de Defensa.*

wsoto@congreso.gob.pe
www.congreso.gob.pe

Edificio Fernando Belaúnde Terry - Jirón Huallaga N° 368, Oficina 302 – Lima
Central Telefónica: 311-7777 Anexo: 7218

salvaguardar sistemas informáticos, aplicaciones, dispositivos, datos financieros y personales frente a diversas amenazas, como el ransomware, las estafas de phishing y el robo de datos. Según la Organización de Estados Americanos (OEA), el ransomware es una de las mayores amenazas cibernéticas en América Latina, cuyo impacto incluye la paralización de sistemas críticos, la pérdida de datos sensibles y el incremento de costos operativos para las víctimas (OEA, 2020)[4].

De igual manera, la Estrategia Nacional de Ciberseguridad del Perú 2017-2021 destaca la importancia de prevenir y mitigar las ciberamenazas para garantizar la estabilidad económica y la seguridad nacional. Estas ciberamenazas no solo afectan a las entidades gubernamentales, sino también a las empresas privadas y a los ciudadanos, quienes a menudo se enfrentan a estafas, suplantación de identidad y acceso no autorizado a sus datos personales (Gobierno del Perú, 2017)[5].

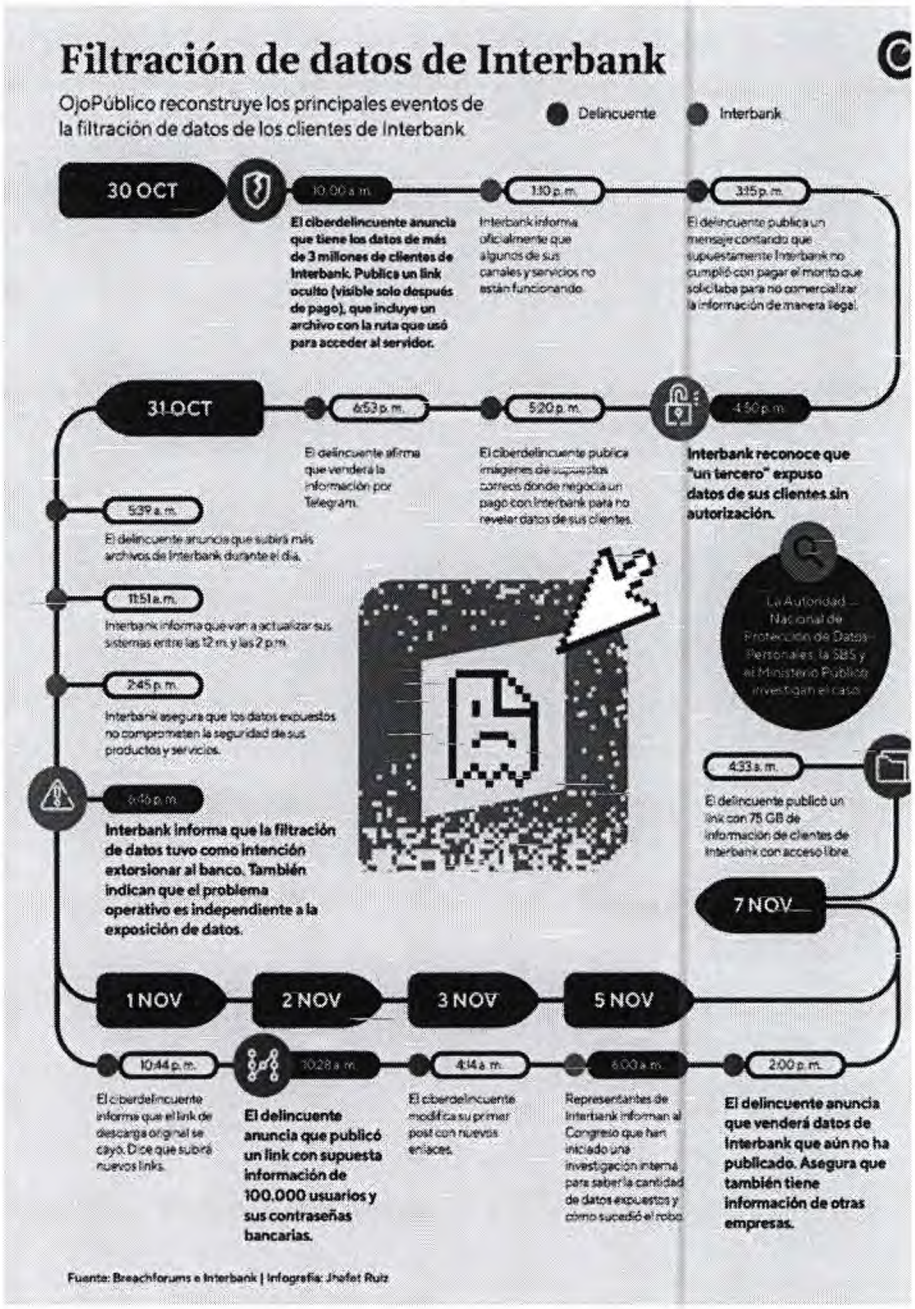
Un claro ejemplo de la creciente amenaza de la ciberdelincuencia ocurrió el 30 de octubre de 2024, cuando se produjo la filtración de datos personales de algunos clientes de Interbank. Ante este incidente, diversas instituciones tomaron medidas: el Indecopi destacó la importancia de que los bancos informen de manera clara y oportuna sobre las acciones para proteger la información de los usuarios; la SBS supervisa las medidas correctivas implementadas por el banco y evaluará posibles infracciones conforme a la normativa vigente; la Autoridad Nacional de Protección de Datos Personales (ANPD) del Ministerio de Justicia inició una fiscalización de oficio para verificar las medidas técnicas y organizativas aplicadas en la gestión de datos personales; y la Fiscalía de Ciberdelincuencia de Lima Centro abrió diligencias preliminares para investigar posibles delitos informáticos. Por su parte, Interbank pidió disculpas a sus clientes, implementó medidas adicionales de seguridad para proteger los depósitos y productos financieros, y comunicó que algunos de sus canales operativos están temporalmente afectados mientras trabajan para restablecer la normalidad[6].

[4] *Organización de Estados Americanos (OEA). (2020).* Informe sobre Ciberseguridad en América Latina. *Washington D.C.: OEA.*
[5] *Idem*
[6] https://www.infobae.com/peru/2024/10/30/indecopi-inicio-monitoreo-a-interbank-por-fallas-operativas-banco-confirmo-filtracion-de-datos-de-usuarios/

wsoto@congreso.gob.pe
www.congreso.gob.pe

Edificio Fernando Belaúnde Terry - Jirón Huallaga N° 368, Oficina 302 – Lima
Central Telefónica: 311-7777 Anexo: 7218

Otro medio reveló detalles del robo de datos en Interbank, exponiendo cómo el atacante accedió a información sensible de clientes del banco. Según expertos consultados, estos accesos suelen estar restringidos a un grupo reducido de empleados y proveedores, lo que hace inusual que el hacker compartiera los archivos, que estuvieron disponibles en línea por poco tiempo antes de ser retirados. El reglamento de la Ley de Protección de Datos Personales exige a las entidades financieras controlar el acceso a sus bases de datos y reportar incidentes a la Autoridad Nacional de Protección de Datos Personales, algo que, según *OjoPúblico*, Interbank no cumplió. Mientras tanto, usuarios reportaron interrupciones en los servicios financieros y notificaciones de movimientos bancarios sospechosos, mientras el banco confirmaba que la información fue robada



wsoto@congreso.gob.pe
www.congreso.gob.pe

Edificio Fernando Belaúnde Terry - Jirón Huallaga N° 368, Oficina 302 – Lima
Central Telefónica: 311-7777 Anexo: 7218

para extorsión. Ante esto, Interbank suspendió sus servicios temporalmente para actualizar sus sistemas, afirmando que estos ataques reflejan una problemática global que afecta al sector financiero pese a los altos estándares de seguridad. El informe también recuerda casos previos de filtraciones en Perú, como la venta de datos del Reniec y Sunarp en 2022, atribuida a credenciales del Ministerio de Energía, y una sanción a la PNP en 2021 por la filtración de antecedentes policiales, evidenciando la necesidad de mayor control en la gestión de bases de datos[7].

La presente propuesta legislativa tiene como propósito fortalecer la seguridad informática en el Perú, enfrentando las conductas ilícitas que buscan acceder, dañar o sustraer información digital perteneciente a personas naturales y jurídicas de derecho público y privado. Este desafío se magnifica frente al incesante avance del desarrollo tecnológico y la creciente sofisticación de los ciberataques dirigidos tanto al Estado como a empresas y ciudadanos.

En este contexto, se hace indispensable la conformación de entidades especializadas encargadas de diseñar y ejecutar mecanismos efectivos de protección. Tal como señala el informe de McAfee (2021), "los ciberataques pueden adoptar diversas formas, incluyendo malware, ataques de denegación de servicio distribuido (DDoS), ransomware y suplantación de identidad, entre otros. Una estrategia sólida de ciberseguridad, acompañada del uso de software confiable, puede reducir significativamente el riesgo de comprometer bases de datos empresariales o personales" (McAfee, 2021)[8].

La preocupación por los ciberataques y su capacidad para vulnerar sistemas informáticos ha llevado a numerosos países a desarrollar regulaciones específicas en materia de ciberseguridad. Estas normativas promueven la colaboración entre organismos gubernamentales, entidades privadas y especialistas, quienes asumen la tarea de controlar posibles infiltraciones por parte de delincuentes cibernéticos, cuyas ubicaciones y operaciones son notoriamente difíciles de rastrear (Kshetri, 2020)[9].

[7] https://www.infobae.com/peru/2024/11/11/robo-de-datos-en-interbank-al-descubierto-asi-opero-el-hacker-para-sustraer-informacion-de-clientes-del-banco/
[8] *McAfee. (2021). El Impacto de los Ciberataques en las Organizaciones. Informe anual.*
[9] *Kshetri, N. (2020). Cybersecurity in the Global Context. En Global Cybersecurity. Springer.*

El sustento de esta propuesta radica en los dictámenes de los Proyectos de Ley N° 4237/2018-CR y N° 4352/2018-CR, "Ley de Ciberseguridad", aprobados el 22 de julio de 2019 por la Comisión de Defensa Nacional, Orden Interno y otras instancias legislativas. Además, se han tomado en cuenta las observaciones formuladas por el Poder Ejecutivo mediante el Oficio N° 244-2019-PR, del 11 de septiembre de 2019, para afinar los alcances y objetivos de la presente iniciativa legislativa.

Por ello, la presente propuesta legislativa busca establecer un marco normativo que permita alcanzar una seguridad informática efectiva, capaz de resistir conductas ilícitas destinadas a vulnerar los sistemas digitales y la información almacenada en ellos. Esta iniciativa se fundamenta en la necesidad urgente de crear entidades especializadas que desarrollen mecanismos de protección, así como políticas públicas orientadas a la prevención, detección y respuesta frente a los ciberataques.

En un entorno caracterizado por el avance incontrolable de las tecnologías digitales y la creciente sofisticación de los ataques cibernéticos, resulta imperativo que el Perú adopte medidas proactivas para proteger tanto los sistemas informáticos del Estado como los de las empresas públicas y privadas, así como los de las personas naturales. Solo mediante la colaboración entre el sector público, el privado, la academia y la sociedad civil será posible construir un ecosistema de ciberseguridad que garantice el desarrollo sostenible y la confianza en las tecnologías digitales (Instituto Nacional de Estándares y Tecnología [NIST])[10].

En ese, la creciente dependencia de las tecnologías digitales y la acelerada evolución de las amenazas cibernéticas exigen una respuesta estratégica y coordinada que garantice la protección de la información y sistemas informáticos en todos los niveles. Incidentes como la reciente filtración de datos en Interbank evidencian la vulnerabilidad de entidades públicas y privadas frente a la sofisticación de los ciberataques, subrayando la necesidad de fortalecer los marcos normativos y las capacidades de ciberseguridad en el Perú. Esta propuesta legislativa no solo busca establecer un marco robusto para prevenir, detectar y responder a estas amenazas, sino también promover la colaboración entre el Estado, el sector privado, la academia y la sociedad civil. De esta manera, se contribuirá a construir un ecosistema digital resiliente y seguro que

[10] *Instituto Nacional de Estándares y Tecnología (NIST). (2021). Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg, MD: NIST.*

impulse el desarrollo económico y social del país, al tiempo que se protegen los derechos fundamentales de las personas frente a los riesgos inherentes de la era digital.

II. EFECTOS DE LA VIGENCIA DE LA NORMA

La presente iniciativa legislativa se encuentra plenamente alineada con la Constitución y el marco jurídico nacional vigente, fortaleciendo la protección de los derechos fundamentales frente a las crecientes amenazas cibernéticas. Su objetivo central es salvaguardar los bienes y la información tanto de las personas como del Estado, promoviendo un entorno digital seguro y confiable que fomente la confianza en las tecnologías y su adopción.

Este marco normativo ofrece herramientas legales y organizativas para que ciudadanos, instituciones públicas y privadas puedan proteger de manera efectiva sus activos digitales e información sensible. Al hacerlo, no solo se impulsa la seguridad en el entorno digital, sino también el desarrollo económico, social y tecnológico del país.

La propuesta también incluye el desarrollo de una reglamentación específica que garantice la implementación eficaz de la norma, estableciendo lineamientos operativos, atribuciones, procedimientos y mecanismos para las entidades especializadas que se crearán en su marco.

En consecuencia, esta norma refuerza y amplía el marco legal existente, dotando al Estado de mayores capacidades para proteger derechos fundamentales en un entorno digital cada vez más complejo. Además, fortalece la confianza ciudadana en las instituciones públicas y privadas, contribuyendo a un desarrollo sostenible, seguro y armonioso en todos los niveles.

III. ANÁLISIS COSTO BENEFICIO

El presente Proyecto de Ley no implica una carga financiera significativa para el Estado, ya que su principal objetivo es regular la seguridad en el uso de herramientas tecnológicas y fomentar la creación de dependencias especializadas. Estas entidades estarán integradas por profesionales del sector público y especialistas del sector privado, trabajando bajo un enfoque colaborativo. En muchos casos, los miembros de estas dependencias cumplirán funciones ad honorem, lo que contribuye a reducir los costos operativos.

wsoto@congreso.gob.pe
www.congreso.gob.pe

Edificio Fernando Belaúnde Terry - Jirón Huallaga N° 368, Oficina 302 – Lima
Central Telefónica: 311-7777 Anexo: 7218

En caso de requerirse recursos adicionales para garantizar el funcionamiento eficiente de las dependencias o comités creados, estos serán cubiertos con los presupuestos ya asignados a las entidades estatales involucradas. Este enfoque permite optimizar los recursos existentes, evitando asignaciones presupuestarias extraordinarias y asegurando la sostenibilidad financiera de la propuesta.

El balance entre los costos mínimos de implementación y los beneficios tangibles y sostenidos justifica plenamente la aprobación del Proyecto de Ley. Al reforzar la seguridad cibernética, se protege a los ciudadanos, se fortalece la confianza en las instituciones, se impulsa el desarrollo económico y se garantiza la estabilidad en un entorno digital en constante evolución, beneficiando a todos los sectores de la sociedad.

IV. VICULACION CON EL ACUERDO NACIONAL

Con la política 7. Erradicación de la violencia y fortalecimiento del civismo y de la seguridad ciudadana.

Nos comprometemos a normar y fomentar las acciones destinadas a fortalecer el orden público y el respeto al libre ejercicio de los derechos y al cumplimiento de los deberes individuales.

Con la Política 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 d los servicios públicos.

Con la política 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 tratados internacionales sobre la materia.

wsoto@congreso.gob.pe
www.congreso.gob.pe

Edificio Fernando Belaúnde Terry - Jirón Huallaga N° 368, Oficina 302 – Lima
Central Telefónica: 311-7777 Anexo: 7218