



PROYECTO DE LEY QUE PROPONE LA CREACIÓN DE LA SUPERINTENDENCIA NACIONAL DE TRANSFORMACIÓN Y SEGURIDAD DIGITAL

El grupo parlamentario **HONOR Y DEMOCRACIA**, a iniciativa del Congresista de la República, **JOSÉ ERNESTO CUETO ASERVI**, ejerciendo el derecho de iniciativa legislativa que le confiere el artículo 107° de la Constitución Política del Perú, y en el inciso c) del Artículo 22°, 67°, 75° y 76° del Reglamento del Congreso de la República, presenta el siguiente Proyecto de Ley:

FÓRMULA LEGAL:

LEY QUE PROPONE LA CREACIÓN DE LA SUPERINTENDENCIA NACIONAL DE TRANSFORMACIÓN Y SEGURIDAD DIGITAL

Artículo 1.- Objeto

La presente ley tiene por objeto crear la Superintendencia Nacional de Transformación y Seguridad Digital como organismo autónomo de derecho público, con la finalidad de conducir, promover y supervisar el proceso de transformación y seguridad digital en el país, en armonía con los marcos normativos vigentes sobre gobierno digital, economía digital, confianza digital e inteligencia artificial.

Artículo 2.- Creación y naturaleza jurídica

La Superintendencia Nacional de Transformación y Seguridad Digital se crea como Organismo Público Técnico Especializado adscrito a la Presidencia del Consejo de Ministros, con personería jurídica de derecho público interno y autonomía técnica, funcional, económica, presupuestal y administrativa, para el ejercicio de sus funciones. Constituye pliego presupuestal y ejerce competencia a nivel nacional, con sede principal en la ciudad de Lima y capacidad para descentralizar sus operaciones según sea necesario.

Artículo 3.- Finalidad

La Superintendencia Nacional de Transformación y Seguridad Digital es el ente rector del Sistema Nacional de Transformación y Seguridad Digital. Su finalidad es garantizar una gobernanza ética, inclusiva y descentralizada de las tecnologías digitales, fomentando el

desarrollo nacional sostenible mediante la promoción del ejercicio pleno de la ciudadanía y democracia digital, el fortalecimiento ético e inclusivo de la industria tecnológica nacional, y la generación de impactos positivos en servicios públicos esenciales, protección de derechos fundamentales y desarrollo económico, social y ambiental.

Tiene a su cargo la conducción de la Política Nacional de Transformación y Seguridad Digital, así como la responsabilidad de promover, diseñar, dirigir, coordinar, supervisar, fiscalizar y evaluar los procesos de transformación y seguridad digital del Estado, el desarrollo de la economía digital, el fortalecimiento del marco de confianza digital, la protección de datos personales, la transparencia en el uso de tecnologías digitales y la gobernanza de la inteligencia artificial en el país.

Artículo 4.- Funciones

La Superintendencia tiene a su cargo las siguientes funciones:

- a) Conducir la Política Nacional de Transformación y Seguridad Digital.
- b) Promover, diseñar, dirigir, coordinar, supervisar, fiscalizar y evaluar los procesos de transformación y seguridad digital en el Estado.
- c) Desarrollar la economía digital y fortalecer el marco de confianza digital.
- d) Proteger datos personales, asegurar transparencia en el uso de tecnologías digitales y gobernar la inteligencia artificial.
- e) Liderar la ciberseguridad nacional, incluyendo la elaboración y actualización de estrategias nacionales contra amenazas cibernéticas, la coordinación de respuestas a incidentes a través de un Centro Nacional de Operaciones de Seguridad (CSIRT nacional), la promoción de estándares de ciberseguridad en entidades públicas y privadas, y la realización de simulacros y evaluaciones periódicas de vulnerabilidades en infraestructuras críticas.
- f) Supervisar y fiscalizar el cumplimiento de normas de protección de datos personales y ciberseguridad, emitiendo certificaciones de cumplimiento, realizando auditorías preventivas y correctivas, y colaborando con autoridades judiciales en investigaciones de delitos informáticos.
- g) Emitir normas técnicas, lineamientos y regulaciones en materia de su competencia, incluyendo protocolos para el manejo seguro de datos sensibles, guías para la implementación de cifrado y autenticación multifactor, y marcos para la resiliencia cibernética en sectores clave como salud, educación y finanzas.
- h) Administrar registros nacionales relacionados con transformación digital, como

identidades digitales y certificaciones, así como bases de datos de incidentes cibernéticos y amenazas reportadas para análisis predictivo y prevención.

i) Imponer sanciones por infracciones a la normativa vigente, clasificadas como leves, graves y muy graves, con multas, suspensiones o cancelaciones según corresponda.

j) Proponer al Poder Ejecutivo y al Congreso de la República políticas y modificaciones normativas.

k) Publicar informes anuales sobre el estado de la transformación digital y rankings de cumplimiento.

k) Celebrar convenios de cooperación con entidades públicas, privadas e internacionales.

l) Otras funciones asignadas en el reglamento.

Artículo 5.- Definiciones

Para efectos de la presente ley, se entiende por:

a) Transformación digital: El proceso de integración de tecnologías digitales en todas las áreas de la sociedad, el Estado y la economía para mejorar la eficiencia, la inclusión, la innovación y la prestación de servicios públicos centrados en el ciudadano, en cumplimiento de los principios de interoperabilidad, accesibilidad y sostenibilidad.

b) Seguridad digital: El conjunto de medidas, políticas y prácticas destinadas a proteger la información, los sistemas, las infraestructuras digitales y las infraestructuras críticas contra amenazas cibernéticas, garantizando la confidencialidad, integridad, disponibilidad y resiliencia de los datos y servicios digitales.

c) Confianza digital: El marco normativo, técnico y ético que fomenta la adopción segura, accesible e interoperable de tecnologías digitales, incluyendo la inteligencia artificial, garantizando la protección de datos personales, la transparencia algorítmica, la ciberseguridad y el respeto a los derechos fundamentales.

d) Gobernanza de la inteligencia artificial: El conjunto de principios, normas y mecanismos establecidos en la normativa vigente sobre inteligencia artificial, destinados a garantizar el desarrollo y uso ético, responsable, transparente, no discriminatorio y explicable de sistemas de inteligencia artificial, minimizando riesgos, previniendo sesgos algorítmicos y maximizando beneficios sociales, en armonía con los derechos fundamentales y los intereses nacionales.

e) Ciberseguridad: El conjunto de estrategias, políticas, herramientas y acciones destinadas a prevenir, detectar y responder a incidentes que comprometan la seguridad de los sistemas, redes y datos digitales, garantizando la continuidad de los servicios y la protección de las infraestructuras críticas.

f) Infraestructura crítica digital: Los sistemas, redes y activos digitales esenciales para la continuidad de los servicios públicos, la seguridad nacional y el funcionamiento de la economía, cuya interrupción o compromiso generaría impactos significativos en la sociedad."

g) Identidad digital: El conjunto de datos electrónicos que identifican de manera única a una persona natural o jurídica en entornos digitales, garantizando su autenticación, seguridad y privacidad en la interacción con servicios digitales.

h) Sesgo algorítmico: La distorsión o resultado no deseado en los sistemas de inteligencia artificial derivado de datos, diseño o implementación que pueda generar discriminación, exclusión o impactos negativos en los derechos fundamentales de las personas.

Artículo 6.- Principios rectores

La Superintendencia Nacional de Transformación y Seguridad Digital actúa conforme a los siguientes principios:

- 1. Inclusión digital.** - Se garantiza que todas las personas, sin distinción, accedan y se beneficien de las tecnologías digitales, reduciendo brechas y promoviendo alfabetización y accesibilidad.
- 2. Equidad algorítmica.** - Se asegura que los algoritmos y sistemas de inteligencia artificial operen sin sesgos ni discriminación, promoviendo resultados justos para todos los grupos sociales.
- 3. Soberanía tecnológica.** - Se fomenta el control y desarrollo autónomo de tecnologías digitales nacionales, reduciendo la dependencia externa y protegiendo datos e infraestructuras críticas.
- 4. Interoperabilidad estatal.** - Se facilita la comunicación e integración de sistemas digitales del Estado para optimizar servicios públicos y evitar duplicidades.
- 5. Seguridad digital:** Se protege la información, sistemas e infraestructuras digitales

contra amenazas, garantizando confidencialidad, integridad, disponibilidad y resiliencia.

- 6. Protección de datos personales.-** Se garantiza el uso lícito, consentido y seguro de la información personal, respetando el derecho fundamental a la privacidad.
- 7. Transparencia en el uso de tecnologías digitales.-** Se asegura que el desarrollo y uso de tecnologías digitales sea claro, comprensible y responsable, informando a los ciudadanos sobre su funcionamiento y decisiones.

Artículo 7.- Organización

La estructura orgánica básica de la Superintendencia comprende:

- a) Consejo Directivo como órgano superior de dirección.
- b) Superintendente como máxima autoridad ejecutiva.
- c) Órganos de línea, administración interna y apoyo.

El Reglamento detallará la estructura orgánica, atribuciones y procedimientos.

Artículo 8.- Consejo directivo

El Consejo Directivo es el órgano máximo de la Superintendencia, responsable de aprobar políticas institucionales y asegurar su adecuada marcha. Está integrado por siete miembros:

- a) El Superintendente, quien lo preside.
- b) Un representante de la Dirección Nacional de Inteligencia, designado por la Presidencia del Consejo de Ministros.
- c) Un representante del Ministerio de Defensa.
- d) Un representante del Ministerio del Interior.
- e) Tres miembros seleccionados por concurso público meritocrático, al menos uno debe ser del sector académico y uno del privado.

Los miembros del Consejo Directivo, con excepción del Superintendente, perciben dietas por las sesiones en que participan, aprobadas de conformidad con lo dispuesto en el Texto Único Ordenado de la Ley 28411, Ley General del Sistema Nacional de Presupuesto.

Los requisitos generales para ser miembro del Consejo Directivo son:

- Ser peruano de nacimiento,
- Mayor de 35 años
- Tener título profesional y grado de maestro o doctor.

- Tener 10 años de experiencia relevante relacionada a transformación digital, seguridad digital, inteligencia artificial o materias afines.
- Conducta intachable.
- Otros que asigne el reglamento.

El período es de cinco años, renovable por única vez.

Los ciudadanos seleccionados son designados por un periodo de cinco (5) años, en la forma prevista en el Reglamento de Organización y Funciones, con opinión favorable de la Presidencia del Consejo de Ministros. Todos los miembros del Consejo Directivo son designados mediante resolución suprema refrendada por el Presidente del Consejo de Ministros.

Los ciudadanos seleccionados mediante concurso público, deberán cumplir con alguno de los siguientes requisitos:

- a) Contar con el grado académico de Doctor y un mínimo de 10 (diez) años como Docente Principal en asignaturas sobre transformación digital, seguridad digital, inteligencia artificial o materias afines, ó
- b) Contar con el grado académico de Doctor, habiéndolo obtenido con estudios presenciales y un mínimo de 10 (diez) años de experiencia en el campo de la investigación y el desarrollo de las ciencias y el conocimiento, con investigaciones y publicaciones en revistas científicas indexadas sobre transformación digital, seguridad digital, inteligencia artificial o materias afines, ó
- c) Contar con el grado académico de Doctor o Maestro y haber desempeñado cargos de gestión en el ámbito público o privado o en el ámbito educativo, por un periodo mínimo de 10 (diez) años en transformación digital, seguridad digital, inteligencia artificial o áreas afines.

El concurso para la selección de miembros del Consejo Directivo otorga el puntaje máximo en la etapa correspondiente, a los candidatos que hayan obtenido el grado de Doctor, a tiempo completo y dedicación exclusiva.

En ningún caso se podrá seleccionar a los tres ciudadanos integrantes del Consejo Directivo bajo el mismo requisito.

Los ciudadanos seleccionados se encuentran sujetos a lo dispuesto por el Código de Ética de la Función Pública.

Todos los miembros del Consejo Directivo deben ser personas de reconocido prestigio y de conducta intachable públicamente reconocida.

Artículo 9.- Funciones del Consejo Directivo

Las funciones del Consejo Directivo son las siguientes:

- a) Proponer la política y lineamientos técnicos en el ámbito de su competencia.
- b) Aprobar los planes, políticas, estrategias institucionales y condiciones básicas de calidad y seguridad digital.
- c) Aprobar, cuando corresponda, sus documentos de gestión.
- d) Supervisar el cumplimiento de objetivos y la implementación del Sistema Nacional de Transformación y Seguridad Digital.
- e) Otros que le asigne el reglamento.

El Consejo Directivo constituye la única instancia administrativa en los casos que sean sometidos a su conocimiento. Las resoluciones que expida son precedentes de observancia obligatoria en los casos que interprete de modo expreso y con carácter general, el sentido de la normativa bajo su competencia

Artículo 10.- Causales de vacancia

Son causales de vacancia del cargo de miembro del Consejo Directivo, las siguientes:

- a) Fallecimiento.
- b) Incapacidad permanente.
- c) Renuncia aceptada.
- d) Impedimento legal sobreviniente a la designación.
- e) Remoción en caso de falta grave debidamente comprobada, conforme a lo dispuesto en los documentos de gestión de la Superintendencia.
- f) Inasistencia injustificada a tres (3) sesiones consecutivas o cinco (5) no consecutivas del Consejo Directivo en el periodo de seis (6) meses, salvo licencia autorizada.

Artículo 11.- Superintendente

El Superintendente de la Superintendencia Nacional de Transformación y Seguridad Digital es la máxima autoridad ejecutiva de la entidad y titular del pliego presupuestal. Es designado mediante Resolución Suprema a propuesta del Presidente del Consejo de Ministros, por un período de cinco años, renovable por un único periodo adicional. El Superintendente continúa en el ejercicio del cargo mientras no se designe a su sucesor. El ejercicio del cargo es remunerado y a tiempo completo.

Para ser designado Superintendente, además de los requisitos establecidos en el artículo 7, se requiere:

1. Acreditar experiencia no menor de diez años en cargos directivos vinculados a la

transformación digital, la seguridad digital, la inteligencia artificial o áreas afines en el sector público o privado.

2. No tener inhabilitación vigente para contratar con el Estado ni para el ejercicio de la función pública en el momento de ser postulado para el cargo.
3. Gozar de conducta intachable públicamente reconocida.

Tiene iniciativa en la formación de leyes en las materias de su competencia. Sus funciones son:

- a) Representar a la Superintendencia
- b) Ejecutar las políticas y realizar las acciones necesarias para la correcta aplicación de los lineamientos técnicos aplicables al servicio en materia de transformación y seguridad digital que sean de su competencia.
- c) Aprobar las normas de regulación del funcionamiento interno de la entidad.
- d) Cumplir y hacer cumplir los acuerdos del Consejo Directivo, emitiendo las Resoluciones de Superintendencia correspondientes.
- e) Designar y remover a los jefes de los órganos de línea y de administración interna de la Superintendencia.
- f) Informar anualmente al Congreso de la República sobre el estado del sistema y comparecer ante este cada vez que sea requerido.
- g) Otras que asigne el reglamento.

Artículo 12.- Régimen de infracción y sanciones

La Superintendencia está facultada para imponer sanciones administrativas por el incumplimiento de las normas en materia de transformación digital, seguridad digital, protección de datos personales, ciberseguridad, confianza digital e inteligencia artificial. Las infracciones se clasifican en leves, graves y muy graves, considerando factores como la intencionalidad, el daño causado, la reincidencia y el impacto en derechos fundamentales o infraestructuras críticas.

- a) Infracciones leves: Incluyen omisiones menores en reportes, incumplimientos formales en protocolos de seguridad no críticos o retrasos en la implementación de lineamientos sin causar daños. Sanciones: Amonestación escrita o multas de hasta 50 Unidades Impositivas Tributarias (UIT).
- b) Infracciones graves: Incluyen violaciones a la protección de datos personales que afecten a un grupo limitado de personas, incumplimientos en estándares de ciberseguridad que expongan vulnerabilidades moderadas, o falta de transparencia en algoritmos de IA con impacto medio. Sanciones: Multas de 51 a 500 UIT, suspensión temporal de actividades digitales por hasta 6 meses, o

revocación de certificaciones.

- c) **Infracciones muy graves:** Incluyen brechas de datos masivas, ataques cibernéticos facilitados por negligencia, uso discriminatorio de IA que vulnere derechos fundamentales, o sabotaje a infraestructuras críticas. Sanciones: Multas de 501 a 5000 UIT, suspensión indefinida o cancelación permanente de licencias, y remisión a autoridades judiciales para posibles acciones penales.

El procedimiento sancionador será regulado en el Reglamento de Infracciones y Sanciones, garantizando el derecho a la defensa, la notificación oportuna, la presentación de descargos en un plazo de 15 días hábiles, y la resolución motivada por el Superintendente.

Las sanciones podrán ser apeladas ante el Consejo Directivo en primera instancia y ante el Poder Judicial en segunda instancia. En casos de reincidencia, las multas se incrementarán en un 50% por cada infracción subsiguiente. Los ingresos por multas se destinarán al fortalecimiento de la Superintendencia.

Artículo 13.- Régimen económico y laboral

La Superintendencia administra su presupuesto con autonomía, priorizando eficiencia y transparencia. Sus recursos son los siguientes:

- a) Asignaciones presupuestales
- b) Ingresos por servicios prestados (como certificaciones y supervisiones)
- c) Donaciones no reembolsables y otros permitidos por ley.

El personal de la Superintendencia se rige por el régimen laboral de la actividad privada, con énfasis en la meritocracia y la capacitación continua en tecnologías digitales.

Artículo 14.- Coordinación descentralizada

La Superintendencia Nacional de Transformación y Seguridad Digital impulsa la cooperación y articulación con gobiernos regionales y locales para implementar políticas de transformación y seguridad digital, en cumplimiento de los principios de descentralización e inclusión digital. Para ello, establece mecanismos de coordinación intersectorial con entidades del Poder Ejecutivo y de cooperación intergubernamental con gobiernos regionales y locales, con los siguientes objetivos:

- Asegurar la ejecución coordinada de las funciones bajo su competencia en los ámbitos nacional, regional y local.
- Implementar sistemas de seguimiento, supervisión, evaluación y monitoreo, con indicadores de gestión para la mejora continua de las políticas digitales.
- Celebrar convenios interinstitucionales de asistencia técnica y promover

acciones de cooperación y colaboración mutua.

Estos mecanismos serán detallados en el Reglamento de la presente ley.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. – Reglamentación

El Poder Ejecutivo aprueba, dentro de un plazo máximo de ciento ochenta (180) días calendario contados a partir de la entrada en vigor de esta ley, el Reglamento de Organización y Funciones, el Reglamento de Infracciones y Sanciones, y demás normas complementarias de la Superintendencia Nacional de Transformación y Seguridad Digital, refrendado por el Presidente del Consejo de Ministros.

Segunda. – Absorción de instituciones y funciones

La Superintendencia Nacional de Transformación y Seguridad Digital absorberá las siguientes instituciones y sus funciones relacionadas con transformación digital, gobierno digital, protección de datos, confianza digital, transparencia, ciberseguridad, conectividad e inteligencia artificial:

- a) Secretaría de Gobierno y Transformación Digital (SGTD) de la Presidencia del Consejo de Ministros (PCM).
- b) Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos (MINJUS).
- c) Autoridad Nacional de Transparencia y Acceso a la Información Pública del Ministerio de Justicia y Derechos Humanos (MINJUS).
- d) Programa Nacional de Telecomunicaciones (PRONATEL) del Ministerio de Transportes y Comunicaciones (MTC).

El proceso de absorción se realizará de manera gradual, respetando los derechos laborales de los servidores y evitando duplicidades, conforme al reglamento de la presente ley.

Tercera. – Transferencia progresiva de funciones

La adecuación institucional para la transferencia de funciones, competencias, recursos y órganos del Poder Ejecutivo hacia la Superintendencia Nacional de Transformación y Seguridad Digital se establecerá mediante decreto supremo refrendado por el Presidente del Consejo de Ministros, conforme a lo dispuesto en la Ley Orgánica del Poder Ejecutivo y demás normas de desarrollo constitucional.

Cuarta. - Previsión presupuestaria:

El financiamiento de las funciones asignadas a la Superintendencia Nacional de Transformación y Seguridad Digital se realiza con cargo a los recursos existentes en los pliegos presupuestales correspondientes, sin demandar recursos adicionales al Tesoro Público, conforme lo que disponga el Ministerio de Economía y Finanzas.

Quinta. - Comisión instaladora

Se crea una Comisión Instaladora temporal, integrada por cinco miembros designados por Resolución Suprema refrendada por el Presidente del Consejo de Ministros, para supervisar la implementación inicial de la Superintendencia en un plazo de 90 días. La Comisión estará presidida por un experto en transformación digital y velará por la transferencia de funciones, recursos y personal, respetando derechos laborales.

Esa Comisión establecerá un plan detallado de absorción para evitar conflictos de competencias y garantizar la continuidad de las funciones transferidas, en conformidad con la segunda disposición complementaria final.

Sexta. - Alineación de la Ley N°31814

La Superintendencia alineará sus funciones de gobernanza de Inteligencia Artificial con la Ley N° 31814 y su Reglamento, asegurando la implementación ética y responsable de la inteligencia artificial.

Séptima. - Vigencia

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

Lima, octubre de 2025



Firmado digitalmente por:
MONTOLYA MANRIQUE Jorge
Carlos FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 21/10/2025 09:27:29-0500



Firmado digitalmente por:
MONTOLYA MANRIQUE Jorge
Carlos FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 21/10/2025 09:27:14-0500



Firmado digitalmente por:
CUETO ASERVI Jose Ernesto
FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 21/10/2025 09:40:24-0500



Firmado digitalmente por:
PADILLA ROMERO Javier
Rommel FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 21/10/2025 13:17:16-0500



Firmado digitalmente por:
ACUÑA PERALTA Segundo
Hector FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 21/10/2025 10:15:38-0500



Firmado digitalmente por:
ECHAIZ RAMOS VDA DE NUÑEZ
Gladys Margot FAU 20161740126
soft
Motivo: Soy el autor del
documento
Fecha: 21/10/2025 17:17:59-0500

I. EXPOSICIÓN DE MOTIVOS

1.1 OBJETO Y FINALIDAD

La presente propuesta legislativa busca crear la Superintendencia Nacional de Transformación y Seguridad Digital como organismo autónomo de derecho público, con personería jurídica de derecho público interno y autonomía técnica, administrativa, económica y funcional. Su finalidad es conducir la Política Nacional de Transformación y Seguridad Digital y ejercer la rectoría del Sistema Nacional de Transformación y Seguridad Digital, conforme al marco normativo vigente, promoviendo el desarrollo de la economía digital, fortaleciendo el marco de confianza digital y liderando la gobernanza de la inteligencia artificial. Además, se orienta a garantizar el ejercicio pleno de la ciudadanía y democracia digital, fomentar el desarrollo ético e inclusivo de la industria tecnológica nacional, y generar impactos positivos en los servicios públicos esenciales, la protección de los derechos fundamentales y el desarrollo económico, social y ambiental del país.

1.2 ANTECEDENTES

El proceso de transformación digital constituye un eje estratégico para el desarrollo económico, social y ambiental del Perú. Desde la promulgación del Decreto Legislativo N.º 1412 – Ley de Gobierno Digital y de la Política Nacional de Transformación Digital (desde ahora PNTD), aprobada mediante Decreto Supremo N.º 118-2023-PCM, se han impulsado políticas públicas orientadas a la digitalización de los servicios del Estado, la economía digital y la confianza digital. Sin embargo, estas iniciativas se encuentran actualmente dispersas entre distintas entidades de la administración pública, lo que limita su eficacia, sostenibilidad y continuidad.

A nivel comparado, países como Estonia, Corea del Sur y Uruguay han institucionalizado órganos de alto nivel, con autonomía y mandato específico, para conducir sus procesos de transformación digital, logrando avances significativos en competitividad, seguridad digital y democracia electrónica.

La transformación digital es un pilar esencial para el desarrollo integral del país, alineado con el Plan Estratégico de Desarrollo Nacional al 2050 (PEDN 2050) y la PNTD. El PEDN 2050 enfatiza un desarrollo equitativo, incluyendo a poblaciones

vulnerables en el acceso a tecnologías digitales y protegiéndolas de riesgos. Su Objetivo Nacional 4 busca una administración pública eficiente, transparente e inclusiva, priorizando accesibilidad y conectividad en zonas rurales y urbanas.

La PNTD define una visión hacia la era digital con seis objetivos prioritarios:

- (1) Garantizar el acceso inclusivo, seguro y de calidad al entorno digital a todas las personas, enfocándose en cerrar la brecha de acceso a internet, con especial atención a poblaciones vulnerables (por género, lengua, discapacidad, entre otras);
- (2) Vincular la economía digital a los procesos productivos sostenibles del país, integrando tecnologías digitales en actividades productivas y promoviendo la inclusión financiera (pagos digitales, digitalización de MIPYMES);
- (3) Garantizar la disponibilidad de servicios públicos digitales inclusivos, predictivos y empáticos con la ciudadanía, incrementando la interacción digital entre el Estado y las personas a través de servicios accesibles, centrados en el usuario y basados en datos;
- (4) Fortalecer el talento digital en todas las personas, desarrollando competencias y habilidades digitales en la población, con énfasis en grupos en situación de riesgo y fomentando una mayor participación de mujeres en tecnología;
- (5) Consolidar la seguridad y confianza digital en la sociedad, fortaleciendo la ciberseguridad y protegiendo especialmente a niños, niñas y adolescentes frente a los riesgos del entorno digital; y
- (6) Garantizar el uso ético y la adopción de las tecnologías exponenciales y la innovación en la sociedad, promoviendo el aprovechamiento responsable de tecnologías emergentes como la inteligencia artificial, el Internet de las Cosas o la impresión 3D, en beneficio del desarrollo social y económico.

En suma, la PNTD brinda el marco estratégico que orienta la transformación digital hacia un entorno inclusivo, seguro e innovador.

II. REALIDAD PROBLEMÁTICA

2.1 BRECHAS ESTRUCTURALES EN EL DESARROLLO DIGITAL DEL PAÍS

El Perú enfrenta brechas estructurales que limitan la transformación digital:

- a) **Fragmentación institucional:** las competencias en gobierno digital, economía digital, inteligencia artificial y confianza digital se encuentran distribuidas en diversos sectores, sin un ente rector con autoridad y capacidad de articulación a nivel nacional y descentralizado.
- b) **Déficit de gobernanza ética y de seguridad digital:** la rápida evolución tecnológica demanda un marco de control, supervisión y regulación que garantice la protección de datos personales, la equidad algorítmica y la soberanía tecnológica.
- c) **Falta de continuidad y estabilidad:** Cambios gubernamentales generan discontinuidad, debilitando competitividad y confianza.

Estas limitaciones afectan servicios públicos, inclusión social e integración a la economía digital global, lo cual lleva al siguiente diagnóstico clave:

- a) **Brecha de acceso a internet y desigualdad digital:** en el primer trimestre de 2025, el 58,9% de hogares tiene acceso a internet (INEI), con disparidad urbano-rural: 79,2% en Lima Metropolitana vs. cifras menores en provincias, limitando inclusión en servicios, educación y oportunidades económicas.
- b) **Fragmentación en gobernanza digital:** Entidades como la Secretaría de Gobierno y Transformación Digital (SGTD) de la Presidencia del Consejo de Ministros (PCM), las Autoridades Nacionales de *Protección de Datos Personales* y de *Transparencia y Acceso a la Información Pública* del Ministerio de Justicia (MINJUS) y el *Programa Nacional de Telecomunicaciones (PRONATEL)* para la conectividad rural del Ministerio de Transportes y Comunicaciones (MTC) e incluso autoridades competentes en firmas digitales, generan duplicidades. La SGTD ha logrado avances, como reglamentación de normas y posicionamiento de Perú como líder regional en tres dimensiones del Índice de Gobierno Digital OCDE 2023, pero su dependencia del Ejecutivo limita transversalidad y sostenibilidad.
- c) **Seguridad digital y ciberdelincuencia:** En 2024, se reportaron 42.000 denuncias por delitos informáticos (aumento del 40% vs. 2023, Ministerio Público) y más de

45 mil millones de intentos de ciberataques (Fortinet). No existe una autoridad integral para liderar respuestas coordinadas.

- d) **Riesgos emergentes:** Junto con la ciberdelincuencia, surgen como la exposición de menores de edad a contenidos nocivos o delitos en línea, la utilización de criptomonedas y plataformas digitales en el lavado de activos y delitos financieros y los riesgos éticos y de seguridad en el uso de la Inteligencia Artificial (IA).

Las causas principales de estos problemas son las siguientes:

- e) **Fragmentación normativa:** diversos marcos legales y órganos han surgido para atender componentes específicos (gobierno digital, conectividad, protección de datos, transparencia, ciberseguridad, etc.), sin una instancia única que los aglutine. Por ejemplo, la Ley de Gobierno Digital (Decreto Legislativo N.º 1412 de 2018) estableció bases importantes para la digitalización del Estado (creación de la entonces Secretaría de Gobierno Digital y obligación de planes de gobierno digital), pero su implementación ha recaído solo en la SGTD como órgano dependiente de PCM. Paralelamente, la Ley de Protección de Datos Personales (Ley 29733) encargó dicha materia al MINJUS (vía la Dirección de Datos Personales como autoridad nacional); la Ley de Transparencia creó otra autoridad en el mismo ministerio para acceso a información pública; la Estrategia Nacional de Seguridad Digital involucra al Ministerio de Defensa e Interior en ciberdefensa; y el PRONATEL en el MTC gestiona proyectos de conectividad. Esta proliferación de actores con mandatos parcialmente traslapados ha llevado a un ecosistema normativo complejo, con *silos* institucionales que dificultan una ejecución coherente. No existe un liderazgo central unificado con suficiente jerarquía para alinear todas estas iniciativas bajo una visión común, lo que conlleva esfuerzos duplicados, lagunas de responsabilidad y menor impacto de las políticas públicas digitales.
- f) **Limitada jerarquía y continuidad de la autoridad actual:** La SGTD, ente rector vigente, carece de autonomía orgánica y rango legal elevado. Al depender directamente de la Presidencia del Consejo de Ministros (PCM), involucrando su estabilidad y capacidades con las decisiones del gobierno de turno. Esta fragilidad institucional se traduce en falta de poder coercitivo para exigir cumplimiento de estándares digitales a otros sectores, dificultades para asegurar presupuesto multianual propio, e incluso riesgo de discontinuidad ante cambios políticos.

Asimismo, la SGTD tiene competencias limitadas para ejercer rectoría sobre gobiernos regionales y locales, lo que ha generado dificultades en la articulación multinivel de la transformación digital. Esto responde a un diseño normativo que no dotó al ente rector de las facultades transversales ni la independencia necesarias para coordinar todos los niveles de la administración pública. Por tanto, una causa de fondo es la débil institucionalidad asignada a la gobernanza digital: hasta ahora no se la ha elevado a prioridad de Estado con respaldo legal, restándole eficacia y peso político.

- g) **Brechas estructurales:** existe insuficiente infraestructura de conectividad, particularmente en zonas rurales y de Amazonía, con geografías complejas y alto costo de despliegue), y la brecha de talento digital es amplia en el sector público y población general. Aunque existe la *Estrategia Nacional de Talento Digital*, la formación de competencias no ha escalado al ritmo requerido: muchas entidades carecen de personal capacitado en gestión de proyectos tecnológicos, ciencia de datos, ciberseguridad o IA. Esto dificulta la adopción efectiva de innovaciones.
- h) **Régimen legal disperso y desfasado:** Si bien en años recientes se han promulgado normas relevantes como la Ley de Gobierno Digital, Ley de Protección de Datos, Ley de Delitos Informáticos, Ley de IA, etc., el marco legal sigue rezagado frente al avance tecnológico acelerado. Por un lado, existen áreas sin regulación específica o con vacíos (por ejemplo, uso de *big data* en la administración pública, computación en la nube, identidad digital como derecho fundamental, etc.). Por otro lado, la ausencia de una autoridad integradora dificulta expedir normativa técnica unificada (estándares de interoperabilidad, seguridad de la información, accesibilidad web, entre otros), lo cual genera heterogeneidad entre entidades. Además, la dispersión legal conduce a posibles incoherencias o conflictos: por ejemplo, la normativa de transparencia obliga publicidad de datos que la normativa de protección de datos podría restringir; o las competencias de ciberseguridad están repartidas entre la Policía (delitos informáticos), el Ministerio de Defensa (ciberdefensa) y la SGTD (seguridad digital), sin claridad absoluta en algunos ámbitos. Todo ello señala la necesidad de fortalecer y actualizar el marco normativo de manera integral, tarea difícil de lograr sin una instancia con mandato global en transformación digital.

Estas causas sistémicas requieren reorganizar la institucionalidad digital para un despliegue coherente y seguro. El Perú enfrenta una encrucijada: cuenta con estrategias como PEDN 2050 y PNTD, pero brechas y fragmentación limitan beneficios.

La ausencia de una autoridad nacional con mandato integral ha dificultado *escalar* los logros obtenidos por la SGTD hacia una política de Estado sostenida y transversal. De continuar así, existe el riesgo de que el país no pueda mantener el ritmo de la revolución digital global, comprometiendo su competitividad, la seguridad de sus ciudadanos en línea y el ejercicio efectivo de derechos fundamentales en la era digital.

2.2 JUSTIFICACIÓN

Para abordar las causas raíz, se propone crear la Superintendencia Nacional de Transformación y Seguridad Digital como organismo autónomo con autonomía plena, rector del Sistema Nacional de Transformación y Seguridad Digital. Su mandato incluye conducir la política digital, desarrollar la economía digital, gobernar la inteligencia artificial y promover la ciudadanía digital, y contaría con las siguientes características

- a) **Enfoque integral:** lo que le permitirá consolidar funciones dispersas para eliminar fragmentación, simplificando el marco organizacional y mejorando eficiencia.
- b) **Autonomía:** Lo que garantizaría decisiones técnicas independientes, asegurando continuidad más allá de cambios gubernamentales.
- c) **Especialización:** La Superintendencia debe operar bajo principios de alta especialización, transparencia y autonomía, lo que permitirá dotar de recursos para políticas de vanguardia, promoviendo innovación y alineando con estándares OCDE.
- d) **Fortalecimiento de la seguridad digital:** Se abordaría de manera unificada los desafíos críticos de ciberseguridad, protección de datos e IA que hoy están fragmentados. Una entidad especializada puede desarrollar estrategias nacionales integrales de ciberseguridad, coordinando con fuerzas del orden, sector privado y comunidad internacional para prevenir ciberataques, proteger infraestructuras críticas y responder eficazmente a incidentes. Igualmente, concentrará la experiencia para garantizar la protección de la información sensible y los datos personales de la ciudadanía, algo fundamental en la era del *big data*. También liderará la formulación de políticas ante tecnologías emergentes como lineamientos para el uso ético y responsable de la Inteligencia Artificial, mitigando riesgos y

potenciando sus beneficios en sectores como salud, educación o seguridad pública.

- e) **Fortalecimiento de derechos digitales:** se fortalecería la protección efectiva de derechos fundamentales en entornos digitales, como el acceso a Internet, la identidad digital y la protección de datos personales, en concordancia con la Constitución y el marco normativo vigente.

2.3 INSUFICIENCIA DE SOLUCIONES VIGENTES

Antes de optar por la creación de una superintendencia autónoma, se han considerado y aplicado diversas alternativas normativas e institucionales para impulsar la transformación digital en el Perú, las cuales resultan insuficientes:

- a) **Alternativa 1:** Mantener el esquema actual (SGTD y múltiples entidades dispersas). No resuelve la fragmentación ni brinda independencia, por lo cual persiste la vulnerabilidad de retrocesos ante cambios gubernamentales y discontinuidad de políticas.
- b) **Alternativa 2: Fortalecer dimensiones específicas** como la ciberseguridad vía ley especializada. Las propuestas legislativas previas no lograron establecer un enfoque integral ni garantizar la autonomía funcional que hoy se plantea con la creación de la Superintendencia, la cual aborda la ciberseguridad, la transformación digital del Estado, la economía digital, la confianza digital y la gobernanza de la inteligencia artificial, de forma coordinada y con capacidad sancionadora, reguladora y de rectoría nacional.
- c) **Alternativa 3: Dejar la transformación digital al mercado o a políticas aisladas.** Si bien no se ha planteado formalmente, cabría la postura de que la innovación digital fluya espontáneamente mediante iniciativas privadas o esfuerzos descentralizados de cada entidad pública. Sus consecuencias serían negativas: la brecha digital podría ampliarse (el mercado por sí solo no conectará a zonas rurales remotas sin incentivos estatales), la seguridad digital estaría descoordinada y la calidad de los servicios públicos digitales dependería de la capacidad individual de cada organismo, acentuando desigualdades, contraviniendo las políticas nacionales vigentes que demandan un rol proactivo del Estado en transformación digital.

Después de evaluar las alternativas mencionadas, resulta claro que solo una reforma integral como la propuesta puede atender integralmente el problema.

2.4 OBJETIVOS DE LA REFORMA PROPUESTA

Los objetivos son los siguientes:

- a) Consolidar gobernanza digital bajo entidad única, unificando competencias.
- b) Garantizar continuidad como política de Estado con estabilidad legal.
- c) Fortalecer capacidad estatal ante riesgos tecnológicos.
- d) Acelerar cumplimiento de PNTD y metas PEDN 2050.
- e) Optimizar recursos públicos, eliminando redundancias.
- f) Empoderar ciudadanía digital y mejorar servicios públicos.

Los objetivos definidos abarcan desde la reforma institucional interna (integración y eficiencia del aparato estatal) hasta los resultados finales esperados en la sociedad (ciudadanos conectados, seguros y aprovechando la tecnología). Cada objetivo contribuye a solucionar los distintos aspectos del problema público identificado, y en conjunto delinean una transformación profunda hacia un Estado Peruano digital, competitivo, seguro e inclusivo.

2.5 IMPACTO ESPERADO

Los principales impactos esperados son:

Eficiencia estatal - reducción de trámites y burocracia: Se espera una reducción de los tiempos y trámites administrativos gracias a la estandarización e interoperabilidad de sistemas que la Superintendencia impulsará. Asimismo, la toma de decisiones en políticas digitales será más rápida al eliminar dilaciones por coordinación interinstitucional prolongada.

Inclusión digital - aceleración de conectividad rural: Se prevé una aceleración en la expansión de la conectividad de internet en comunidades rurales. Al tener el mandato legal de garantizar el derecho de acceso a Internet, la Superintendencia priorizará proyectos de última milla, centros de acceso digital comunitario y alianzas público-privadas para llevar conexión a donde el mercado no llega. El impacto esperado es que en algunos años el porcentaje de hogares con internet se incremente sustancialmente (por ejemplo, superar el 80% de hogares conectados a nivel nacional en el mediano plazo, reduciendo drásticamente la brecha urbano-rural). Esto redundará en mayor igualdad de oportunidades.

Seguridad y confianza digital: Con la Superintendencia unificando la estrategia de seguridad digital, se espera implementar un Sistema Nacional de Alerta y Respuesta a Incidentes Cibernéticos más eficaz, coordinando a todas las entidades públicas y sector privado crítico. Esto debe traducirse en menor cantidad de incidentes graves (brechas de datos masivas, ataques exitosos a infraestructura crítica) o, en su defecto, en una respuesta más inmediata y efectiva cuando ocurran, minimizando daños. También aumentará la confianza del público en transacciones digitales: al contar con una entidad que certifique estándares de seguridad y supervise el cumplimiento de la Ley de Protección de Datos, los ciudadanos tendrán mayor certeza de que sus datos personales están resguardados adecuadamente en bases de datos estatales y privadas.

Economía digital: En el corto plazo, la Superintendencia impulsará la digitalización de MIPYMEs articulando iniciativas de capacitación y plataformas de comercio electrónico accesibles, lo que puede elevar la productividad de estas unidades. Un impacto esperado es el crecimiento de la economía digital como proporción del PIB, dado que actividades como el comercio electrónico, los servicios de tecnología financiera (fintech) y la industria de desarrollo de software/local *startups* tendrán un entorno más propicio (menos trabas burocráticas digitales, más seguridad jurídica).

Democracia digital: La Superintendencia también influirá en cómo se relacionan ciudadanos y Estado en la era digital, fortaleciendo la democracia. Un impacto previsto es el aumento de canales de participación ciudadana digital (consultas en línea, presupuestos participativos virtuales, plataformas de colaboración), ampliando la voz de la ciudadanía en la toma de decisiones públicas. Del mismo modo, mayor transparencia proactiva en formato de datos abiertos y portales unificados de información, que faciliten el control social y la rendición de cuentas.

Internacional: Con esta reforma, el país se alinearán con las mejores prácticas globales de gobernanza digital, lo que acelerará su ingreso a la OCDE y cumplimiento de diversos compromisos internacionales. Perú pasaría a ser visto como referente regional en transformación digital de la administración pública, similar a naciones líderes como Uruguay o Estonia en sus respectivas regiones. Esto abre puertas a cooperación internacional, transferencia tecnológica y liderazgo en iniciativas multinacionales sobre gobierno digital, inteligencia artificial ética y protección de datos transfronterizos, entre otros.

La reforma propicia Estado eficiente, sociedad conectada y economía dinámica. Los beneficios superan a los costos transitorios.

III. ANÁLISIS DE IMPACTO NORMATIVO

El proyecto es conforme con la Constitución Política del Perú:

- **Artículo 43**, establece que el Estado es unitario y descentralizado.
- **Artículo 44**, que fija como deber esencial del Estado promover el bienestar general y garantizar la plena vigencia de los derechos humanos.
- **Artículo 102 inciso 1**, que atribuye al Congreso la facultad de dar leyes y velar por el respeto de la Constitución.

Es coherente con el Código Civil, que en sus artículos 75 y 76 reconocen la personería jurídica de derecho público interno, necesaria para la Superintendencia Nacional de Transformación y Seguridad Digital.

Es coherente con leyes especiales como:

- Ley N.° 1412 – Ley de Gobierno Digital.
- Ley N.° 27658 – Ley Marco de Modernización de la Gestión del Estado.
- Políticas y lineamientos emitidos por el Poder Ejecutivo sobre economía digital, confianza digital e inteligencia artificial.

La reforma propuesta no deroga estas normas, sino que les otorga un marco legal de mayor jerarquía y estabilidad.

VIABILIDAD JURÍDICA, POLÍTICA Y ADMINISTRATIVA DE LA REFORMA

La propuesta es viable en los siguientes ámbitos:

- a) **Jurídica:** viable, fortalece estructura estatal sin vulnerar principios constitucionales; alineada con compromisos OCDE.
- b) **Política:** alineada con Acuerdo Nacional (Políticas 9, 20, 24); responde a agenda legislativa 2023-2024.
- c) **Administrativa:** transición ordenada, aprovechando recursos existentes; respeta legalidad y competencias preexistentes vía transferencia gradual.

IV. ANÁLISIS COSTO BENEFICIO

Los costos son la adecuación organizacional inicial para la instalación de la nueva Superintendencia y la asignación presupuestal para su funcionamiento, que puede provenir de recursos actualmente dispersos en distintos sectores.

Los beneficios son los siguientes:

- a) Eficiencia y reducción de duplicidades en políticas y proyectos de transformación digital.
- b) Mayor seguridad digital y fortalecimiento de la confianza de ciudadanos y empresas.
- c) Estabilidad institucional, al quedar la Superintendencia protegida de los vaivenes políticos.
- d) Incremento de la competitividad nacional, atracción de inversiones y promoción de la industria tecnológica.

Se puede sintetizar el análisis costo-beneficio en la siguiente tabla comparativa:

Horizonte	Costos (principales)	Beneficios Directos (ejemplos)	Beneficios Indirectos (ejemplos)
Corto Plazo	- Reorganización inicial de entidades, integración de sistemas). - Esfuerzo político y administrativo de transición. - Posible resistencia al cambio en algunos sectores.	- Rápida eliminación de duplicidades (ahorro administrativo). - Mejora inmediata en trámites clave (ventanilla única, más servicios en línea). - Implementación acelerada de proyectos prioritarios (ej. identidad digital nacional).	- Señal positiva a inversionistas y socios internacionales (mayor confianza en el país). - Acceso expedito a cooperaciones y financiamiento externo para agenda digital. - Mayor satisfacción ciudadana inicial por simplificación de trámites y coherencia en políticas.

Largo Plazo	- Mantenimiento de la entidad (presupuesto anual consolidado). - Adaptación continua a nuevas tecnologías (inversión permanente en actualización). - Riesgo de burocratización si no se gestiona adecuadamente (debe evitarse).	- Estado altamente eficiente: ahorro sostenible de costos operativos (trámites 100% digitales, menos papel, menos tiempo). - Servicios públicos de calidad mundial, accesibles a toda la población (100% de localidades conectadas, todos los ciudadanos con identidad digital). - Mayor seguridad digital: reducción significativa de incidentes cibernéticos exitosos, protección efectiva de datos personales.	- Incremento del crecimiento económico (por productividad digital, impulso a industria tecnológica). - Reducción de brecha social: comunidades rurales con mismas oportunidades digitales que urbanas, disminución de desigualdad regional. - Democracia fortalecida: ciudadanía empoderada digitalmente, participación masiva en procesos democráticos en línea, mayor transparencia y control social.
-------------	---	---	---

Tabla 1: Comparativa de costos y beneficios de la creación de la Superintendencia Nacional de Transformación y Seguridad Digital, diferenciando impactos a corto y largo plazo.

En términos globales, el análisis demuestra que los beneficios proyectados superan ampliamente a los costos. Los costos identificados son manejables y en su mayoría transitorios, mientras que los beneficios son de gran magnitud y permanentes en el tiempo. Por ejemplo, el costo de implementar la reforma se ve sobrepasado por beneficios anuales recurrentes (ahorros económicos, mejoras de bienestar) que una vez alcanzados se sostienen indefinidamente.

Cabe recalcar que este análisis, aunque fundamentado, debe refinarse con estudios técnicos detallados durante la implementación. Se recomienda que la Autoridad, una vez creada, realice evaluaciones ex post para medir exactamente los ahorros logrados y los impactos, a fin de retroalimentar sus estrategias. No obstante, con la información disponible y la lógica de mejora de procesos, es razonable concluir que la reforma es económicamente conveniente para el país.

El balance neto es favorable, dado que la reorganización y centralización de competencias generará ahorros y mejores resultados en el mediano y largo plazo.

V. EFECTOS DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

La creación de la Superintendencia Nacional de Transformación y Seguridad Digital:

- a) Fortalece el Sistema Nacional de Transformación Digital, otorgando rango legal a la conducción de la política en la materia.
- b) Exige la aprobación de un Reglamento que desarrolle su estructura y funciones, integrando las normas vigentes en gobierno digital, economía digital, confianza digital e inteligencia artificial.
- c) No produce conflictos con la legislación actual; proporciona un marco jerárquico que da coherencia y estabilidad a las normas ya existentes.

CONTRIBUCIÓN A LAS POLÍTICAS NACIONALES Y COMPROMISOS INTERNACIONALES

La propuesta de crear la Superintendencia Nacional de Transformación y Seguridad Digital contribuye directamente a las políticas nacionales vigentes y a los compromisos internacionales del Perú en materia digital, fortaleciendo la implementación de estrategias clave para el desarrollo tecnológico inclusivo y seguro.

Política Nacional de Transformación Digital (PNTD) y sus seis objetivos prioritarios

La PNTD establece seis objetivos prioritarios que guían la transformación digital del país. La Superintendencia actuará como ente rector para su materialización, asegurando coordinación y recursos sostenidos. Para el acceso inclusivo (Objetivo 1), liderará proyectos de conectividad rural, alianzas con operadores privados y campañas de seguridad, cerrando brechas urbano-rurales y protegiendo a vulnerables. En economía digital (Objetivo 2), simplificará trámites para MIPYMEs, fomentará comercio electrónico y promoverá inclusión financiera, integrando tecnologías en sectores productivos como agro y manufactura para impulsar competitividad sostenible.

Para servicios públicos digitales (Objetivo 3), desarrollará plataformas transversales como identidad y firma digital, exigiendo digitalización en entidades públicas con enfoque centrado en el usuario y uso de IA predictiva, logrando cobertura nacional.

En talento digital (Objetivo 4), impulsará capacitaciones para funcionarios y ciudadanía, con énfasis en mujeres, discapacitados y adultos mayores, elevando competencias generales. Finalmente, para seguridad y confianza (Objetivo 5) e innovación ética (Objetivo 6), fortalecerá ciberdefensa, protección de datos y regulación de IA/IoT, protegiendo menores y fomentando adopción responsable de tecnologías emergentes.

Este alineamiento aumenta la probabilidad de cumplir la PNTD al 2030, con rendición de cuentas ante el Congreso para monitoreo efectivo.

Plan Estratégico de Desarrollo Nacional al 2050 (PEDN 2050) en materia digital

El PEDN 2050 aspira a un Perú desarrollado con equidad, donde la transformación digital es transversal. La Superintendencia alineará la institucionalidad digital con sus metas, priorizando conectividad universal para cerrar brechas territoriales mediante infraestructura de fibra óptica, redes satelitales y cobertura total al 2030, posicionando la conectividad como servicio básico. En educación y sociedad del conocimiento, apoyará plataformas virtuales, dotación tecnológica en escuelas y formación en STEM, asegurando alfabetización digital universal al 2050.

Para sectores productivos, impulsará IA e IoT en agroindustria, minería y servicios, mejorando productividad y sostenibilidad. En ciudadanía y descentralización, creará nodos regionales para políticas locales adaptadas, homogenizando capacidades digitales y fomentando smart cities, reforzando cohesión nacional y equidad territorial.

La Superintendencia es clave para transitar de planificación a ejecución, garantizando avances consistentes hacia la visión de un Estado inteligente y una economía basada en conocimiento.

Cumplimiento de compromisos internacionales (OCDE)

La reforma fortalece el proceso de adhesión a la OCDE, ajustando la gobernanza digital a estándares de países desarrollados. El Índice de Gobierno Digital OCDE 2023 destacó avances peruanos en usuario-centrismo, diseño digital y datos, gracias a la SGTD, pero requiere mayor institucionalidad. La Superintendencia cumple recomendaciones como coordinación central, estrategias centradas en el usuario y gobernanza de datos, acelerando evaluaciones y adhesión.

Otros desafíos clave

También abordará desafíos digitales clave. En ciberdelincuencia, centralizará estrategias con Policía y Ministerio Público para prevención y respuesta, incluyendo protocolos unificados y campañas de concientización. Para lavado de activos digitales, colaborará con la Unidad de Inteligencia Financiera en regulación de fintech y criptomonedas, usando IA para detectar patrones sospechosos.

En protección de menores, integrará políticas educativas con filtros de contenido y denuncias centralizadas, promoviendo entornos seguros. Para riesgos de IA, emitirá lineamientos éticos bajo la Ley N.º 31814, con comités de expertos en aspectos regulatorios, asegurando uso responsable en sectores críticos.

En resumen, la Superintendencia ofrece respuestas coordinadas contra amenazas digitales, convirtiendo riesgos en oportunidades y fortaleciendo confianza en la transformación.

ANÁLISIS COMPARADO DE MODELOS INTERNACIONALES

A nivel global, varios países han creado modelos institucionales innovadores para liderar la transformación digital y la seguridad cibernética, de los cuales el Perú puede extraer lecciones valiosas. A continuación, se resumen algunos casos destacados – de diversas regiones y contextos – señalando su marco normativo, funciones principales y resultados alcanzados:

País	Entidad rectora digital	Nivel normativo	Funciones principales	Resultados destacados
Estonia	Agencia Estatal de Sistemas de Información (RIA)	Agencia gubernamental autónoma (Ley de 2008)	Ciberseguridad, identidad digital, interoperabilidad, servicios en línea.	99% de servicios públicos en línea; 100% población con ID digital; voto electrónico; ahorros ≈2% PIB/año (firmas digitales).
Singapur	Infocomm Media Development Authority (IMDA)	Agencia estatutaria (Ley parlamentaria,	Regulación TIC/medios, impulso de economía y	Líder Asia en gobierno digital; 98% hogares con internet; plataformas nacionales unificadas

		2016)	sociedad digital; protección de datos (PDPC)	(SingPass); alta confianza en uso de datos personales.
Reino Unido	Government Digital Service (GDS)	Unidad central del Gobierno (creada 2011, reorganizada 2024)	Estandarizar y digitalizar servicios públicos; portal GOV.UK; datos y tecnología en gobierno.	Ahorros > £1,700 millones en década; portal único GOV.UK; pionero en diseño centrado en usuario; reformado en 2024 bajo Ministerio de Tecnología.
Corea del Sur	Ministerio del Interior y Seguridad + NIA	Ministerio y agencia pública (políticas continuas desde 1987) (¿Cómo Corea del Sur ha logrado ser pionero en la transformación digital del sector público? - Gobernarte)	Planificación de e-gobierno; infraestructura nacional de información; servicios digitales integrados.	Top 3 mundial en e-gobierno ONU; 95% hogares con internet; portal unificado; 30 años de mejora continua de servicios digitales públicos.
India	Ministerio de Electrónica y TI (MeitY) + UIDAI	Ministerio con programas nacionales (Digital India desde 2015)	Identidad digital (Aadhaar); inclusión digital; digitalización de trámites; pagos digitales masivos.	1.3 mil millones de ciudadanos con Aadhaar (Assessing the Effectiveness and Privacy Implications of Aadhaar ...); >74 mil millones transacciones UPI en 2022 (UPI continues to dominate digital payments thanks to wide use of QR ...); subsidios entregados sin intermediarios; boom startups fintech.

China	Comisión Central de Asuntos del Ciberespacio (CAC)	Órgano central partidario/estat al (desde 2014); Leyes de Ciberseguridad y Datos	Gobernanza integral internet y datos; impulso de economía digital; censura y control contenidos; servicios gubernamentales en línea.	1,067 millones de internautas (75.6% población) (Digital China Development Report (2022) Released, China's Digital Economy Ranks Second in the World); economía digital = 41.5% PIB (Digital China Development Report (2022) Released, China's Digital Economy Ranks Second in the World); >1,000 millones de usuarios en plataforma gubernamental online; liderazgo en 5G/IoT.
Japón	Agencia Digital (Digital Agency)	Agencia gubernamental (creada por ley 2021)	Coordinar transformación digital de todo el gobierno; unificar sistemas; promover e-ID (MyNumber).	+75% población con identificación MyNumber (2023); eliminación de trámites en papel/sellos; integración de sistemas locales; mejora en rankings e-gobierno.

Tabla 2: Modelos internacionales de institucionalidad para la transformación digital y sus logros principales. Fuentes: normativa oficial de cada país y reportes públicos¹, entre otros.

Estos ejemplos internacionales evidencian que no existe un modelo único, pero sí principios comunes de éxito: un liderazgo institucional claro (sea agencia autónoma, ministerio o unidad central) con apoyo político al más alto nivel; mandatos legales firmes que definen competencias en transformación digital y ciberseguridad; y la capacidad de ejecutar proyectos nacionales que generen resultados tangibles (servicios en línea efectivos, ahorros económicos, mayor confianza pública). Además, muestran que los países líderes ajustan su institucionalidad con el tiempo – reubicando, fusionando o creando órganos – según evolucionan sus necesidades tecnológicas.

¹ Business Wire. (2023, 30 de abril). Digital China Development Report (2022) released: China's digital economy ranks second in the world. Business Wire. <https://www.businesswire.com/news/home/20230429005017/en/Digital-China-Development-Report-2022-Released-Chinas-Digital-Economy-Ranks-Second-in-the-World>

La propuesta de crear una Superintendencia Nacional de Transformación y Seguridad Digital se alinea con estas lecciones internacionales, buscando adaptar lo mejor de cada modelo a nuestra realidad.

VI. RELACIÓN DE LA PROPUESTA LEGISLATIVA LAS POLÍTICAS DE ESTADO EXPRESADAS EN EL ACUERDO NACIONAL

La propuesta se alinea con los siguientes objetivos de Políticas de Estado del Acuerdo Nacional:

- **Décima Primera Política de Estado:** Acceso universal a las tecnologías de la información y comunicación.
- **Décima Política de Estado:** Promoción de la competitividad, productividad y empleo.
- **Décima Séptima Política de Estado:** Gobierno eficiente, transparente y descentralizado.

Asimismo, responde a la Agenda Digital del Perú y a los compromisos asumidos en foros internacionales como la OCDE, que promueven la transformación digital como herramienta de desarrollo sostenible.

La creación de la Superintendencia Nacional de Transformación y Seguridad Digital es una respuesta ambiciosa pero proporcional a la dimensión del desafío que enfrenta el Perú en la era digital. Hemos visto que el problema actual – fragmentación institucional, brechas de acceso, amenazas cibernéticas y rezago tecnológico – es de carácter estructural y transversal, afectando al Estado, la economía y la sociedad en su conjunto. Frente a ello, la solución propuesta se erige con la misma magnitud: dotar al país de una entidad autónoma, integral y de máximo nivel legal dedicada a liderar la transformación digital en todos sus frentes. Esta no es una medida desproporcionada, sino más bien alineada con la importancia estratégica de lo digital para el desarrollo nacional y la garantía de derechos fundamentales en el siglo XXI.

La reforma es plenamente viable – jurídica, política y administrativamente – como se ha argumentado. No vulnera la Constitución, sino que la enriquece, al incorporar mecanismos para hacer efectivos nuevos derechos (acceso a internet, protección de

datos, etc.) bajo una institucionalidad sólida. Cuenta con amplio sustento en políticas de Estado ya consensuadas (Acuerdo Nacional) y con precedentes legislativos favorables. Su implementación aprovechará recursos existentes, minimizando costos, y reorganizará eficientemente la administración pública digital. En suma, es una reforma realista y ejecutable, que puede y debe ser puesta en marcha con la planificación adecuada.

Más importante aún, la creación de la Superintendencia Nacional de Transformación y Seguridad Digital es legalmente sólida y necesaria para alcanzar los objetivos que el propio Estado peruano se ha trazado y para hacer frente a los retos del entorno global. Estamos ante un escenario mundial de aceleración tecnológica, donde países y empresas compiten por innovar, y donde también emergen riesgos que trascienden fronteras (ciberataques, desinformación, uso malicioso de la IA, etc.).

El Perú no puede quedarse rezagado ni desprotegido. Se requiere una entidad que empodere institucionalmente al país hacia una verdadera democracia digital, en la que todos los ciudadanos puedan ejercer sus derechos en línea con la misma plenitud que en el mundo físico, donde la tecnología sirva para ampliar la participación y la inclusión, y donde el Estado sea más transparente y cercano gracias a lo digital. Esta reforma empodera al Perú en ese sentido, dándole las herramientas para innovar en sus procesos democráticos (mecanismos de participación virtual, gobierno abierto), manteniendo a la vez el debido resguardo de los derechos y principios constitucionales en el nuevo entorno (libertad de expresión en internet, privacidad, igualdad de acceso).

Asimismo, la reforma responde a los desafíos globales y se anticipa a riesgos emergentes. La Superintendencia propuesta permitirá al Perú cumplir con estándares internacionales (OCDE) y adoptar las mejores prácticas de países líderes, cerrando la brecha que nos separa de ellos.

Se tendrá una entidad capaz de adaptarse continuamente al cambio tecnológico, de modo que cuando surjan nuevas tendencias – desde economías digitales descentralizadas hasta futuras redes o inteligencias artificiales más avanzadas – el Estado peruano cuente con la capacidad instalada para abordarlas proactivamente. Esto es esencial para no reaccionar tarde, sino para moldear el rumbo de la transformación digital de forma soberana, protegiendo el interés nacional. La reforma se anticipa a riesgos latentes: blindamos nuestra soberanía digital (evitando depender fragmentariamente de agendas externas), refuerza la seguridad nacional en el ciberespacio y prepara a nuestra

fuerza laboral y juventud para los empleos del futuro mediante la educación digital.

Finalmente, se trata de simplificar y fortalecer la arquitectura del Estado para dar respuesta a una realidad insoslayable. La transformación digital no es opcional; está ocurriendo a nuestro alrededor y afecta todos los aspectos de la vida. La vinculación con las Políticas de Estado apunta a que, sin un salto cualitativo en nuestra institucionalidad digital, corremos el riesgo de no cumplir nuestras metas de desarrollo, de profundizar brechas sociales y de exponer a nuestra ciudadanía a peligros crecientes en línea.

En cambio, con la Superintendencia Nacional de Transformación y Seguridad Digital, el Perú podrá proteger derechos fundamentales en entornos digitales (como el derecho a la privacidad, a la información, a la educación en línea), garantizando la continuidad de los servicios del Estado ante cualquier adversidad (haciendo nuestra administración resiliente y cercana), coadyuvando a sentar las bases de un crecimiento económico apoyado en la innovación y el conocimiento.